VMware Cloud Director 10.2.2 Release Notes

VMware Cloud Director 10.2.2 | 8 APR 2021 | Build 17855679 (installed build 17855680)

Check for additions and updates to these release notes.

What's in this Document

What's New

VMware Cloud Director version 10.2.2 includes the following:

- **VMware Tanzu Mission Control supports Tanzu Kubernetes clusters provisioned in VMware Cloud Director** - You can attach to Tanzu Mission Control a Kubernetes cluster that is provisioned in VMware Cloud Director. As a result, the cluster becomes visible in the Tanzu Mission Control console. For information about attaching an existing cluster to your VMware Tanzu Mission Control organization, see Attach an Existing Cluster in the *VMware Tanzu Mission Control Product Documentation*.
- **Tanzu Kubernetes Cluster Tenant Network Isolation** - Tanzu Kubernetes clusters are now only reachable from workloads within the same organization virtual data center in which a cluster is created. If necessary, you can manually configure external access to specific services in a Tanzu Kubernetes cluster. For more information, see Configure External Access to a Service in a Tanzu Kubernetes Cluster in the *VMware Cloud Director Tenant Portal Guide*.
- **Tanzu Kubernetes Cluster Pod and Services CIDR selection**- During the creation of a Tanzu Kubernetes cluster, you can specify ranges of IP addresses for Kubernetes services and Kubernetes pods. For more information, see Create a Tanzu Kubernetes Cluster in the *VMware Cloud Director Tenant Portal Guide*.
- **VMware Cloud Director uses its management network for communication with Tanzu Kubernetes Clusters -** The VMware Cloud Director management network is a private network that serves the cloud infrastructure and provides access for client systems to perform administrative tasks on VMware Cloud Director. Earlier releases use the Kubernetes service network.
- **VMware Cloud Director appliance SNMP agent** - You can configure the agent to listen for

polling requests. If there is a preexisting Net-SNMP agent, during the upgrade, the VMware Cloud Director appliance replaces the Net-SNMP installation with VMware-SNMP. During VMware-SNMP setup, the VMware Cloud Director appliance configures dynamically the firewall rules required for SNMP operation. You must remove any existing firewall rules that work with Net-SNMP before the upgrade. For more information, see Configuring the VMware Cloud Director Appliance SNMP Agent in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

- **Global Placement Policy** - Service providers can define placement policies that work effectively across all vCenter Server instances and clusters in a VMware Cloud Director environment. A single placement policy can point to hosts that span multiple clusters in one or more vCenter Server instances. Boundaries in underlying infrastructure are abstracted behind the global logical construct of a placement policy making for a more logical experience for both service providers and tenants. This change enables capturing the placement policy when a vApp template is created from a VM; the resulting vApp template inherits every placement policy from the original VM even if the VM and vApp Template are in different Provider VDCs. Best practice is to use a distinctive naming convention for the placement policies. For more information, see Create a Global VM Placement Policy in the *VMware Cloud Director Service Provider Admin Portal Guide*.
- **Guest Customization for Encrypted VMs** – VMware Cloud Director 10.2.2 supports guest customization of VMs that run on encrypted storage.
- **Organization Virtual Data Center Templates** – You can create and share virtual data center (VDC) templates with tenant organizations so that organization administrators can use the templates to create VDCs. VMware Cloud Director 10.2.2 supports the use of NSX-T based networking with the organization VDC templates.
- **Storage Policy Update** – Service providers can use storage policies in VMware Cloud Director to create a tiered storage offering, for example, Gold, Silver, and Bronze, or even offer dedicated storage to tenants. With the enhancement of storage policies to support VMware Cloud Director entities, you have the flexibility to control how you use the storage policies. You can have not only tiered storage, but isolated storage for running VMs, containers, edge gateways, and so on.

  A common use case that this update addresses is the need for shared storage across clusters or offering lower cost storage for non-running workloads. For example, instead of having a storage policy with all VMware Cloud Director entities, you can split your storage policy into a *Workload Storage Policy* for all your running VMs and containers, and a dedicated *Catalog Storage Policy* for longer term storage. A slower or low cost NFS option can back the *Catalog Storage Policy*, while the *Workload Storage Policy* can run on vSAN.
- **FIPS Support** – This release of VMware Cloud Director includes support for the Federal Information Processing Standards**.** Both the VMware Cloud Director appliance and Linux binary can run in FIPS-compliant mode. FIPS mode is disabled by default and enabling FIPS mode might affect the performance of VMware Cloud Director. If metrics collection is configured, verify the configuration of the server and client communication with Cassandra over SSL. For more information, see Enable or Disable FIPS Mode on the VMware Cloud Director Appliance in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide.* Alternatively*,* for enabling VMware Cloud Director on Linux, see Enable FIPS Mode on the Cells in the Server Group in the *VMware Cloud Director Service Provider Admin Portal Guide*.
- **Direct VDC Networks Support in Organization VDCs backed by NSX-T Data Center**–

  Service providers can create direct organization VDC networks in VDCs backed by NSX-T Data Center

Data Center.

- **Autoscaling** – Scaling groups are a new top level object that tenants can use to implement automated horizontal scale-in and scale-out events on a group of workloads. You can configure auto scale groups with a source vApp template, a load balancer network, and a set of rules for growing or shrinking the group based on the CPU and memory use. VMware Cloud Director automatically spins up or shuts down VMs in a scaling group. See the Auto Scale Groups documentation in the *VMware Cloud Director Tenant Portal Guide*.
- **Guided Tours Update** – Service providers can publish custom-built guided tours and scope the tours to system administrators or tenants. Starting with VMware Cloud Director 10.2.2 you can download guided tours from a VMware Github repository or a custom Github repository.
- **Removing Static T-shirt Size** – VMware Cloud Director 10.2.2 no longer supports the use of the predefined virtual machine sizes available since vCloud Director for Service Providers 9.0. You can use the VM sizing policy functionality to provide predefined VM sizing.

System Requirements and Installation

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

For information on appliance configuration and sizing, see the guidelines inVMware Cloud Provider Pod Designer - VMware Validated Designs for Cloud Providers.

Supported cipher suites enabled by default:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

System administrators can use the cell management tool to explicitly enable other supported cipher suites that are disabled by default.

Note: Interoperation with releases of vCenter Server earlier than 5.5-update-3e and versions of ovftool earlier than 4.2 require VMware Cloud Director to support TLS version 1.0. You can use the cell management tool to reconfigure the set of supported SSL protocols or ciphers. See the Cell Management Tool section in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Deploying the VMware Cloud Director Appliance

In some cases, the vami_firstboot file is not automatically deleted after the deployment of the VMware Cloud Director appliance. Because of this, during the next appliance power cycle or restart, the appliance is reinitialized. To avoid this issue, run the following steps on each appliance in the server group after its deployment.

1. Determine if the file /opt/vmware/etc/vami/flags/vami_firstboot exists on the VMware Cloud Director appliance.
2. If the file exists, run the following command to delete it.

```
rm /opt/vmware/etc/vami/flags/vami_firstboot
```

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 10.2.1 Release Notes

VMware Cloud Director 10.2 Release Notes

Resolved Issues

- **After upgrade to VMware Cloud Director 10.2.x, execution of any CMT command on Cassandra with SSL fails with an error message**
  When you use the cell-management-tool to configure or reconfigure Cassandra with SSL, the operation fails with an error message.
  ```
  Unable to load VCD's SSL context.
  ```
- **New After disabling a VM to join a domain, updating the VM hardware properties fails with an error message**
  If you disable for a VM to join a domain, updating the hardware properties of the same VM fails with an error message.
  ```
  Error: <Domain name> should not be provided when domain join is disabled.
  ```
- **New After enabling a VM to join a domain, updating the VM hardware properties fails with an error message**
  If you configure the Enable this VM to join domain guest customization on a VM, updating the hardware properties of the same VM fails with an error message.
  ```
  Error: <UUID> Domain name, Username, and Password cannot be empty if Join Domain is
    selected
  ```
- **In an organization VDC with the reservation pool allocation model, when you instantiate a vApp from a template, the deployed VMs have incorrect configurations**
  The issue occurs when a VDC with the non-reservation pool allocation model backs a catalog. Storing a vApp template in that catalog and instantiating a vApp from it in an organization VDC with the reservation pool allocation model results in VMs with incorrect configurations for memory reservation and memory limit.
- **Attempting to delete a VM from a vApp immediately after undeploying the same VM fails with an error message**
  When you use the VMware Cloud Director API to delete a VM from a vApp immediately after undeploying the VM, the operation fails with an error message.
  ```
  Failed to delete object.
  ```
- **Imported LDAP users do not have the rights to change the user password but see the Change password option in the Tenant Portal UI**
  In the VMware Cloud Director Tenant Portal, if an imported LDAP user navigates to the top

navigation bar and clicks their user name, the drop-down menu incorrectly displays the **Change password** option even though the user does not have the rights to change the user password.

- **In a vApp that is connected to a direct organization VDC network, you cannot set the IP mode for a virtual machine's NIC to Static - IP Pool**
  In a vApp that is connected to a direct organization VDC network, you cannot set the IP mode for a virtual machine's NIC to `Static - IP Pool`. This occurs if the direct network is backed by an external network with multiple subnets and the first subnet's IP pool is fully utilized. When you add another NIC to the VM, or another VM to the vApp, and set the IP mode to `Static - IP Pool`, VMware Cloud Director does not apply the settings and changes the IP mode to `DHCP`.

- **Attempts to upgrade VMware Cloud Director 10.1.2 to version 10.2.x incorrectly reports an error**
  When you upgrade VMware Cloud Director 10.1.2 to version 10.2.x, the following incorrect error message appears:

  ```
  ERROR: The RPM for another version of VMware Cloud Director is already installed, but that version is not
  recognized and upgrading from that release is not supported. This upgrade is not expected to succeed, but you
  may proceed anyway at your own risk.
  ```

  VMware Cloud Director supports upgrades from version 10.1.2 to version 10.2.x and you can ignore the error message.

- **When you reboot the VMware Cloud Director appliance, the services API or the appliance management UI might report that the vmware-vcd service is in a failed state**
  When you reboot the VMware Cloud Director appliance, the services API or the appliance management UI might mistakenly report that the `vmware-vcd` service is in a failed state. This happens when the `vmware-vcd` service attempts to start before the OS networking stack becomes available. As a result, the service enters a failed state and you see an error message displaying that the service failed to bind to one or more ports. Subsequently, the `vcd-watchdog` starts the `vmware-vcd` service successfully, but the `systemd` service status does not reflect that.

- **Cannot publish a provider VDC Kubernetes policy to a VDC if the Supervisor Cluster it points to is not the primary cluster in the provider VDC**
  If you have a provider VDC with multiple Supervisor Clusters, publishing a provider VDC Kubernetes policy that points to a non-primary Supervisor Cluster fails with an `LMException` error.

- **If a storage pod or a cluster backs a storage policy, you cannot enable VMware Cloud Director IOPS limiting on that storage policy**
  In the Service Provider Admin Portal, when one or more storage pods or clusters back a storage policy, even if you turn off the **Impact placement** flag, you cannot enable VMware Cloud Director IOPS limiting on that storage policy.

- **After you update the Publish Settings of a subscribed catalog from the Tenant Portal UI, synchronizing this catalog fails with a 401 Unauthorized error**
  After you update the **Publish Settings** of a subscribed catalog from the Tenant Portal UI, synchronizing this catalog fails with a `401 Unauthorized` error. This happens because updating

the catalog settings deletes the existing password and sets it to null.

- **When you open the Virtual Machines list in a vApp and you enable the Multiselect option, the Actions menu becomes unavailable**
  When you open the Virtual Machines list in a vApp and you enable the Multiselect option, the Actions menu becomes unavailable. You can select multiple virtual machines, but you cannot perform any action on them simultaneously.

- **When filtering a multi-selection grid, navigating to another page causes the filtered items to disappear**
  In multi-selection grids, if you filter the results and more than one page is available, the next pages of filtered results appear empty. The issue occurs in dialog boxes where you can select multiple items from a list and filter them, for example, adding storage policies to an organization VDC or sharing a vApp or VM to users or groups.

- **When a vApp User attempts to create a vApp from a template, the operation results in "Operation is denied" error message**
  If your assigned user role is vApp User, when you attempt to create a vApp from a template and you customize the VM sizing policies for the virtual machines in the vApp, this results in "Operation is denied" message. This happens because the vApp User role allows you to instantiate vApps from templates, but it does not include rights that allow you to customize a virtual machine's memory, CPU or hard disk. By changing the sizing policy, you change the virtual machine memory or CPU.

- **In the Kubernetes Container Clusters plug-in, data grids might appear empty while loading**
  In the Kubernetes Container Clusters plug-in, some data grids appear empty while loading because the loading spinner does not appear.

- **Using the VMware Cloud Director API to retrieve a host returns incorrect value for the numOfCpusLogical parameter**
  When you run the `GET /admin/extension/host/{id}` API call to retrieve a host, the `NumOfCpusLogical` field displays the number of physical CPUs instead of logical CPUs.
  The issue is fixed in this release by deprecating the `NumOfCpusLogical` field and adding two new fields in the body of the output:
  `NumOfCpuCoresPhysical`
  `NumOfCpuCoresLogical`

- **VMware Cloud Director spikes in the CPU consumption cause system slowdown**
  Some VMware Cloud Director cells show high CPU consumption by the `vcloud` service. The high CPU consumption causes slow cell performance, and some tasks fail.

- **You cannot perform a guest customization on an encrypted virtual machine**
  If you associate a VM with a storage policy that has the VM Encryption capability, enabling the guest customization on the VM does not apply the guest customization configurations.

- **Disabling an NSX-T policy-based IPSec VPN fails with an error message**
  When using the HTML5 UI or the VMware Cloud Director API to disable an NSX-T policy-based IPSec VPN, the operation fails with an `error code 500090` error message.

- **Instantiating a VM from a template does not deploy the VM with the correct**

configuration for network adapter type
When you instantiate a VM from a template, the deployed VM does not retain the correct configuration for network adapter type.

- **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.

- **Trying to log in to VMware Cloud Director when using an LDAP user with a group inherited role fails**
  If you log in as an LDAP user that inherits its role from an LDAP group, the login operation fails with an `Authentication Error` error message.

- **VMware Cloud Director logs you off from all open browser sessions**
  If you open the HTML5 UI in multiple browser windows or tabs and you are not active in all of them for more than the time specified in the **Idle session timeout** configuration, VMware Cloud Director logs you off from all open sessions.

- **When using Chrome browser, clicking a datastore name in the list of all datastores does not open the datastore details page**
  If you open the VMware Cloud Director Service Provider portal in Chrome, clicking a datastore name in the list of all datastores does not open the datastore details page.

- **Updating the name and the description of a security group removes the existing members from the group**
  If you update the name or the description of a security group, the existing members are removed from the group.

- **The Create a vApp from an OVF file wizard displays the product and vendor names as links that link back to the VMware Cloud Director tenant portal**
  When you create a vApp from an OVF package, the **Product** and **Vendor** names in the **Review Details** page of the wizard are displayed as links that direct back to the VMware Cloud Director tenant portal.

- **Creating a vApp from an OVA fails with a Timed out error message**
  When an OVA file is larger than 8 GB, creating a vApp from this OVA file fails with a `Timed out` error message.

- **The Edit group wizard does not display all available tenant roles**
  If your organization consists of more than 15 tenant roles, the **Role** drop-down menu in the **Edit group** wizard displays only 15 roles.

- **After deleting an organization VDC network, update of a firewall rule for an edge gateway fails with an error message**
  If you delete an organization VDC network that is used in a firewall rule for an edge gateway, any subsequent update of another firewall rule for the same edge gateway fails with an error message.
  `Edge firewall source/destination type with value ??virtualwire-xx?? is not recognized and supported by VMware Cloud Director.`

- **The Save button in the Edit Rules wizard is greyed out and you cannot update the**

- **The Save button in the Edit Rules wizard is greyed out and you cannot update the firewall rules**
  If an NSX-T Data Center firewall rule is configured to use a **Reject** action, when you update the firewall rule in the HTML5 UI, the **Save** button in the **Edit Firewall** wizard is greyed out.

- **Powering on a vApp fails with an Invalid state error message**
  If powering on of a vApp takes longer than 3 minutes, the operation fails with an `Invalid state` error message.

- **The internal interface of the NSX Edge gateway is disconnected for a VDC deployed by using a VDC template**
  If you use the VMware Cloud Director API to create a new VDC from a VDC template that includes configurations for a routed network, the internal interface of the deployed NSX Edge is disconnected.

- **The Create Edge Gateway wizard cannot display more than 15 edge clusters available for an organization VDC**
  In an organization VDC configured with more than 15 edge clusters, when deploying a new edge gateway, the **Edge Cluster** page of the **Create Edge Gateway** wizard displays only 15 of the edge clusters.

- **The data grid in the Edit Edge Cluster Assignment appears as blank**
  If you add an edge gateway to a data center group, the data grid in the **Edit Edge Cluster Assignment** wizard appear to be blank.

- **The execution wizard for a vRealize Orchestrator workflow displays the URL of the VDC instead of the VDC name**
  In VMware Cloud Director, when you initiate a vRealize Orchestrator workflow, the **Execute a service** wizard displays the URL of a VDC instead of the VDC name.

- **After upgrade to VMware Cloud Director 10.2, the service monitor reports the Console Proxy endpoint as Unavailable**
  After you upgrade from vCloud Director 9.7 to VMware Cloud Director 10.2, the load balancer service monitor reports the Console Proxy endpoint as **Unavailable,** and an attempt to access the cell fails with an `ERR_CONNECTION_REFUSED` error message.

- **After disabling a VM to join a domain, some operations on the same VM fail with a DomainName should not be provided when domain join is disabled error message**
  If you enable the **Enable this VM to join domain** guest customization for a VM and later disable it, renaming the VM or adding it to a vApp fails with an error message.
  `DomainName should not be provided when domain join is disabled`

Known Issues

- **New Mounting an NFS datastore from NetApp storage array fails with an error message during the initial VMware Cloud Director appliance configuration**
  During the initial VMware Cloud Director appliance configuration, if you configure an NFS datastore from NetApp storage array, the operation fails with an error message.
  `Backend validation of NFS failed with: is owned by an unknown user.`

Workaround: Configure the VMware Cloud Director appliance by using the VMware Cloud Director Appliance API.

- 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 **You cannot edit the LDAP Synchronization settings for your organization**
  On the **LDAP Synchronization Settings** tab in the VMware Cloud Director Service Provider Admin Portal, when you click on **Edit** nothing happens and you cannot edit the LDAP settings for your organization.

  Workaround: None.

- New **VMware Cloud Director displays incorrect value for LDAP synchronization start time**
  In the VMware Cloud Director Service Provider Admin Portal, the LDAP synchronization page displays the date and time of opening the page as **Synchronization Start time** instead of the date and time you configure.

  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 VMware Cloud Director API calls to retrieve vCenter Server information return a URL instead of a UUID**
  The issue occurs with vCenter Server instances that failed the initial registration with VMware Cloud Director version 10.2.1 and earlier. For those vCenter Server instances, when you make API calls to retrieve the vCenter Server information, the VMware Cloud Director API incorrectly returns a URL instead of the expected UUID.

  Workaround: Reconnect to the vCenter Server instance to VMware Cloud Director.

- **New VMware Cloud Director takes longer than the time specified in Idle session timeout configuration to log you off from the HTML5 UI**
  VMware Cloud Director takes twice the time that you specify in the**Idle session timeout** configuration to log you off from the HTML5 UI.

  Workaround: You must minimize the window or switch to another tab in the same window.

- **New 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.

- **New 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
  ```

  Workaround: Run `/opt/vmware/vcloud-director/bin/configure`.

- **New Attempt to upload OpenSSL-generated PKCS8 files to a VMware Cloud Director Appliance in FIPS mode 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 permissions 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 attempt 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 about disabling 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 using the VMware Cloud Director API to apply a priority filter to an advisory, the operation fails with an error message.

  ```
  "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 theVMware 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 order of descending priorities. 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 because the NFS is full, becoming read only, and so on, the appliance cluster functionalities start to malfunction. HTML5 UI is unresponsive while the NFS is down or cannot be reached. Other functionalities that might be affected are 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, if you use the HTML5 UI to log 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 does 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**.
- **Attempt 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.

The Enable Logging toggle is active for an organization administrator role without the

- **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.

  Workaround: This issue is fixed in the VMware Cloud Director 10.2.2.1 patch release.

- **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.