VMware Cloud Director 10.2 Release Notes

VMware Cloud Director 10.2 | 15 OCT 2020 | Build 17029810 (installed build 17008054)

Check for additions and updates to these release notes.

What's in this Document

What's New in This Release

VMware Cloud Director version 10.2 includes the following:

- **NSX-T Advanced Functional Parity:** NSX Advanced Load Balancer (Avi), Distributed Firewall , VRF-lite, Cross VDC networking, IPv6, Dual stack (IPv4/IPv6) on the same network, SLAAC, DHCPv6, CVDS (vSphere 7.0/NSX-T 3.0), L2VPN – API only
- **Support modern applications in VMware Cloud Director with Tanzu runtime vSphere with Kubernetes:** Provider and tenant UI for managing and consuming Kubernetes clusters
- **VMware Cloud Director Virtual Appliance Enhancements:** Validation of user input during initial deployment; Simplified cell restore with streamlined standby cell creation
- **Storage Enhancements:** Disk level IOPS control for providers and tenants; Shared disks
- **Security Enhancements:** See the Security section
- **UI Enhancements:** Quick Search; Advisories; Certificate Management
- **Platform extensibility enhancements**
- **Scale Enhancements:** See VMware Configuration Maximums

For information about the new and updated features of this release, seeWhat's New in VMware Cloud Director 10.2.

For the latest release notes for the VMware Cloud Director add-on solutions, see the following links:

- Container Service Extension 3.0
- Object Storage Extension 2.0
- App Launchpad 2.0
- Terraform
- Tenant App 2.5

Security

VMware Cloud Director 10.2 virtual appliance ships with Photon OS updated up to thisPhoton Security Advisory.

VMware Cloud Director 10.2 supports PKCS12 keystores. You can use a PKCS12 formatted keystore when you configure the network and database connections of VMware Cloud Director, or when you use the cell management tool to generate or replace certificates. For more information, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Product Support Notices

TKG cluster nodes are isolated. However, the services that a TKG cluster exposes are accessible to anyone with network access to the service virtual IP or endpoint and are protected by the services' own authentication and authorization mechanisms. Because authentication is the only protection to secure access to the workloads, it is strongly recommended that you allow only encrypted traffic, such as TLS, on the ingress services.

End of Life and End of Support Warnings

- VMware Cloud Director API version 29 and earlier are not supported.
- VMware Cloud Director API versions 30 and 31 are deprecated.
- VMware Cloud Director API version 30 is due to become unavailable in the next release.
- The /api/sessions API login endpoint is deprecated since VMware Cloud Director API version 33.0/VMware Cloud Director 10.0 and is due to become unsupported in a future VMware Cloud Director release. You can use the separate VMware Cloud Director OpenAPI login endpoints for the service provider and tenant access to VMware Cloud Director.
- The API /cloud/server_status is deprecated for both HTTP and HTTPS protocols. The removal of /cloud/server_status is due in a future VMware Cloud Director release. You must use the/api/server_status for both HTTP and HTTPS protocols.
- The reset actions /amqp/action/resetAmqpCertificate and /amqp/action/resetAmqpKeyStore are removed from VMware Cloud Director API Version 35.0 due to the way VMware Cloud Director stores and handles SSL certificates. You must use the /cloudapi/1.0.0/ssl/trustedCertificates endpoint to untrust certificates.
- The update actions /amqp/action/updateAmqpCertificate and /amqp/action/updateLdapKeyStore are deprecated. The removal of the actions is due in a future VMware Cloud Director release. You can use the new endpoint for trusting of AMQP certificates /cloudapi/1.0.0/ssl/trustedCertificates.
- The reset actions /ldap/action/resetLdapCertificate and /ldap/action/resetLdapKeyStore are removed since VMware Cloud Director API Version 34.0 due to the way VMware Cloud Director 10.1 stores and handles SSL certificates. You must use the /cloudapi/1.0.0/ssl/trustedCertificates endpoint to untrust certificates.
- The update actions /ldap/action/updateLdapCertificate and /ldap/action/updateLdapKeyStore are deprecated and are due to become unsupported in a future release. VMware Cloud Director introduces a new endpoint for

  trusting of LDAP certificates /cloudapi/1.0.0/ssl/trustedCertificates.
- vSphere deprecates the vSphere SSO as a SAML IDP. All VMware Cloud Director deployments configured to use vSphere SSO as their SAML IDP must migrate to a different external SAML IDP. The use of this IDP is due to become unsupported in the next vSphere and VMware Cloud Director releases.
- DSA and DSS certificates are no longer supported because no recommended cipher suites are available for them.

Upgrading from Previous Releases

For more information on upgrading to VMware Cloud Director 10.2, upgrade and migration paths and workflows, see Upgrading and Migrating the VMware Cloud Director Appliance or Upgrading vCloud Director

on Linux.

System Requirements and Installation

Ports and Protocols

For information on the network ports and protocols that VMware Cloud Director 10.2 uses, seeVMware Ports and Protocols.

Compatibility Matrix

See the VMware Product Interoperability Matrixes for current information about:

- VMware Cloud Director interoperability with other VMware platforms
- Supported VMware Cloud Director databases
- NSX Advanced Load Balancer (Avi) - This release of Cloud Director currently only supports NSX Advanced Load Balancer (Avi) version 20.1.1

Supported VMware Cloud Director Server Operating Systems

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

Deploying the VMware Cloud Director Appliance

When you deploy the VMware Cloud Director appliance 10.2 as an OVF template by using the VMware OVF Tool, you must include the following parameter, which is new for version 10.2: --X:enableHiddenProperties. If you do not include this parameter, the VMware OVF Tool fails with a Property vcloudapp.nfs_mount.VMware_vCloud_Director is not user configurable. error.
See Deploying the VMware Cloud Director Appliance by Using VMware OVF Tool

Supported AMQP Servers

VMware Cloud Director uses AMQP to provide the message bus used by extension services, object extensions, and notifications. This release of VMware Cloud Director requires RabbitMQ version 3.8.x.

For more information, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

Supported Databases for Storing Historic Metric Data

VMware Cloud Director supports Apache Cassandra versions 3.11.*x*.

Disk Space Requirements

Each VMware Cloud Director server requires approximately 2100MB of free space for the installation and log files.

Memory Requirements

Please consult *VMware Cloud Director Installation, Configuration, and Upgrade Guide* for memory requirements

CPU Requirements

VMware Cloud Director is a CPU-bound application. CPU over-commitment guidelines for the appropriate version of vSphere should be followed. In virtualized environments, regardless of the number of cores available to VMware Cloud Director, there must be a sensible vCPU to physical CPU ratio, that does not result in extreme over-committing.

Required Linux Software Packages

Each VMware Cloud Director server must include installations of several common Linux software packages. These packages are typically installed by default with the operating system software. If any of the packages are missing, the installer fails with a diagnostic message.

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

In addition to the installer required packages, several procedures for configuring the network connections and creating SSL certificates require the use of the Linux nslookup command, which is available in the Linux bind-utils package.

Supported LDAP Servers

You can import users and groups to VMware Cloud Director from the following LDAP services.

Platform	LDAP Service	Authentication Methods
Windows Server 2012	Active Directory	Simple, Simple SSL
Windows Server 2016	Active Directory	Simple, Simple SSL
Linux	OpenLDAP	Simple, Simple SSL

Supported Security Protocols and Cipher Suites

VMware Cloud Director requires the client connections to be secure. SSL version 3 and TLS version 1.0 and 1.1 have been found to have serious security vulnerabilities and are no longer included in the default set of protocols that the server offers to use when making a client connection. System administrators can enable more protocols and cipher suites. See the Cell Management Tool section in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*. The following security protocols are supported:

- TLS version 1.2
- TLS version 1.1 (deactivatedd by default)
- TLS version 1.0 (deactivatedd by default)

Supported cipher suites enabled by default:

- 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

System administrators can use the cell management tool to explicitly enable other supported cipher suites that are deactivated 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*.

Supported Browsers

VMware Cloud Director is compatible with the current major and previous major release of the following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Note: Internet Explorer 11 is not supported in VMware Cloud Director 10.2 and later. You can use Microsoft Edge or another supported browser. If you must use Internet Explorer 11, consider staying on VMware Cloud Director version 10.0.x or 10.1.x until you can use another browser.

Supported Guest Operating Systems and Virtual Hardware Versions

VMware Cloud Director supports all guest operating systems and virtual hardware versions supported by the ESXi hosts that back each resource pool.

VMware Cloud Director WebMKS 2.1.1

The VMware Cloud Director WebMKS 2.1.1 console adds support for:

- the PrintScreen key in Google Chrome and in Mozilla Firefox for Windows.
- the Windows key in Windows and macOS. To simulate pressing the Windows key, press Ctrl+Windows in Windows OS, or Ctrl+Command in macOS.
- Automatic keyboard layout detection in Google Chrome and Mozilla Firefox.

Resolved Issues

- **Attempting to add a NAT rule to an NSX-T edge gateway fails**
  Attempting to add a NAT rule to an NSX-T edge gateway fails with the error:`New and deprecated values have been updated together for redistribution.`, error code `503266`.

- **Moving a VM across clusters fails if the target storage container is a datastore cluster**
  Moving a VM across clusters fails if the target storage container is a datastore cluster. The logs show the following error.

  2020-05-18 15:51:12,083 | ERROR | task-service-activity-pool-23 | SdrsPlacementManagerImpl | SDRS invocation error | requestId=eaa593e5-e051-4423-ac02-97ad09a39f4c,request=POST https://bos1-vcd-sp-static-203-38.eng.vmware.com/ap

i/vApp/vm-c2b0ee1f-02f1-4377-8852-a9711c2a571e/action/reconfigureVm,requestTime=1589817067877,remoteAddress=10.150.203.38:32049,userAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 ...,accept=application/*+xml;version 3 4.0 vcd=6e36bc7a-3850-4f2a-a057-d96758ef5fbe,task=1e8217b8-88f1-41f8-8292-1bb6178b0b3e activity= (com.vmware.vcloud.backendbase.management.system.TaskActivity,urn:uuid:1e8217b8-88f1-41f8-8292-1bb6178b0b3e) (vmodl.fault.InvalidArgument) { faultCause = null, faultMessage = null, invalidProperty = spec.host }

- **Cannot deploy appliance if the "Expire Root Password Upon First Login" setting is enabled**
  When attempting to deploy an appliance, the deployment fails and the following error is found in the /opt/vmware/var/log/firstboot log:
  Invoking postgresauth script ... sudo: Account or password is expired, reset your password and try again Changing password for root. sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper sudo: unable to change expired password: Authentication token manipulation error cp: cannot stat '/var/vmware/vpostgres/current/.ssh/id_rsa': No such file or directory chown: cannot access '/opt/vmware/vcloud-director/id_rsa': No such file or directory [ERROR] postgresauth script failed to execute.

- **In the VMware Cloud Director Tenant Portal, advanced filtering of VMs based on VDC location does not work**
  In the VMware Cloud Director Tenant Portal UI, if you try to use advanced filtering based on VDC location to filter VMs, the search fails with an error.

Known Issues

- 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 **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 **In the Tenant Portal UI, when you create an affinity or an anti-affinity rule, deselecting the Required check box does not affect the rule configuration**
  In the Tenant Portal UI, when you create an affinity or an anti-affinity rule, deselecting the Required check box does not affect the rule configuration. Affinity and anti-affinity rules are always Required, which means that if a rule cannot be satisfied, the VMs that are added to the rule don't power on.

  Workaround: None.

- 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 **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.

- New **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.

  Workaround: You must have administrator-level access to work around this issue.

  1. In vCenter Server, remove the storage policy tag from all storage pods for which you want to enable IOPS and refresh the storage policies.
  2. In VMware Cloud Director, enable VMware Cloud Director IOPS on the storage policy by turning off the **Impact Placement**.
  3. In vCenter Server, reattach the tag to the storage pods and refresh the storage policies.
- New **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.

  Workaround: None.

- New **You are unable to edit the NIC settings of a standalone virtual machine**
  You are unable to update the NIC settings of a standalone virtual machine. When you click Edit to open the NIC settings of the virtual machine, the settings page opens but becomes unresponsive.

  Workaround:
  1. Convert the standalone virtual machine to a vApp
  2. Edit the NIC settings of the vApp.
  3. Convert the vApp back to a standalone virtual machine.

- New **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 causes the existing password to be deleted and set to null.

  Workaround: Update the **Publish Settings** of the catalog and set the password again from the Tenant Portal UI.

- New **Upgrade of VMware Cloud Director to version 10.2 from version 10.1.2 incorrectly reports an error**
  During the upgrade of VMware Cloud Director to version 10.2 from version 10.1.2, the following inaccurate error message is displayed:

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.

Upgrading VMware Cloud Director to version 10.2 from version 10.1.2 is supported and you must ignore the error message.

Workaround: Ignore the error.

- **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 which reads 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.

  Workaround:

  1. Run `systemctl reset-failed vmware-vcd.service`.
  2. Run `systemctl start vmware-vcd.service`.
- **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 and vCenter Server to version 7.0.0d, 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 Kubernetes endpoint certificate. For detailed steps, see https://kb.vmware.com/s/article/80996.

- **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 deactivate 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: Deactivate manually the vCloud Availability 4.0.0 plug-in.

- **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.

Workaround: Ensure that the provider VDC is backed by only one Supervisor Cluster and that cluster is the primary cluster. A provider VDC can be backed by host clusters and a Supervisor Cluster but the Supervisor Cluster must be the primary.

- **Entering a Kubernetes cluster name with non-Latin characters deactivates 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.

- **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.

  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.

- **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.

  Workaround: Resize any of the columns of the grid.

- **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.

- **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.

- **When a vApp User attempts to create a vApp from a template, this might result in "Operation is denied" 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 could be changing the virtual machine memory or CPU.

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.

- **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 from vCloud Director 10.0, a newly deployed VM from a Linux template with enabled guest OS customization and IPv6 connectivity, experiences network connectivity issues**
  After upgrade from vCloud Director 10.0, if you deploy a new VM by using a Linux VM template created in version 10.0 with enabled guest OS customization and IPv6 connectivity, the deployed VM experiences network connectivity issues. This can happen because the deployment process creates duplicate entries for the `VM_DOMAIN_NAME` and `VM_HOST_NAME` parameters in the VM's `/etc/hosts` file.

  Workaround: Remove the `VM_DOMAIN_NAME` and `VM_HOST_NAME` duplicate entries from the VM's `/etc/hosts`

file.

- **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 organization VDC in which you are deploying it.

  Workaround: None.