Edit document

VMware Cloud Director 10.1 Release Notes

VMware Cloud Director 10.1 | 9 APR 2020 | Build 15967253 (installed build 15967236)

Check for additions and updates to these release notes.

What's in this Document

What's New in This Release

- For information about the new and updated features of this release, see the VMware Technical White Paper What's New with VMware vCloud Director 10.1.
- Changed behavior in the HTML5 UI:
  In earlier VMware Cloud Director versions, you can use the vApp action menu in the HTML UI to stop or to power off a vApp. Both power operations undeploy the vApp, but affect the vApp differently. The Power Off operation does not follow the Start and Stop Order settings for the virtual machines in the vApp. The Power Off operation also undeploys any vApp networks by disconnecting all VM NICs from organization VDC networks and by removing any edge gateways deployed for the vApp.

  In VMware Cloud Director 10.1, performing the Power Off operation on a running vApp results in powering off all the virtual machines in the vApp without undeploying the vApp and the virtual machines in it. The NICs of the virtual machines remain connected to the respective networks and any vApp edge gateways remain deployed. The vApp and the virtual machines in the vApp remain deployed. The Power Off action for each of the individual virtual machines in the vApp remains active and you can use it to power off a virtual machine. This action results in the undeployment of this virtual machine.

  When you power off a vApp, the Power Off operation follows the start order that you defined in the Start and Stop Order settings. As a result, virtual machines are powered off in reverse order to how you configured them for startup. The Stop Wait setting is not applied during the Power Off operation. When you power off a vApp, the power state of the vApp, which is derived from the power states of the virtual machines in it, displays as Powered Off.

- The VMware Cloud Director API 34.0 schema includes definition for the `numberOfCpus` and `MemoryAllocationMB` attributes.

Security

Edit document

- **WARNING:** After upgrading to version 10.1, VMware Cloud Director will always verify certificates for any infrastructure endpoints connected to it. This is due to a change in the way VMware Cloud Director manages SSL certificates. If you do not import your certificates into VMware Cloud Director before the upgrade, the vCenter Server and NSX connections might show failed connection errors due to SSL verification issues. In this case, after upgrading, you have two options:
  1. Run the cell management tool `trust-infra-certs` command to automatically connect and retrieve certificates of all infrastructure endpoints for vCenter Server and NSX Manager instances into the centralized certificate store. See Import Endpoints Certificates from vSphere Resources.
  2. In the Service Provider Admin Portal UI, select each vCenter Server and NSX instance and reenter the credentials while accepting the certificate.

- Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers and to verify server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after a VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Deny List.
- VMware Cloud Director 10.1 deprecates the behavior to trust all SSL certificates. In this release, vCenter Server and NSX connections do not support this option. For all other connections, trusting all certificates is also deprecated and will become unsupported after VMware Cloud Director 10.1. System Administrators must prepare for this transition.
  - If you use the LDAP for your VMware Cloud Director system organization, you can use the trust-on-first-use dialog in the UI or upload certificates by using the API.
  - Audit all uses of this option and supply appropriate certificates by using the UI or the API.
  - Communicate the changes to the tenants. All tenants that are using custom LDAP with enabled **Accept all certificates** option must transition away from this configuration. Tenants can either use the trust-on-first-use dialog in the UI or upload certificates through the API.

Updated Open Source Packages

- Updated `jackson-databind` to version 2.9.10.1.
- Updated `jre` to version 1.8.0u231.
- Updated `openssl` to version 1.0.2u.
- Updated `xstream` to version 1.4.11.1.

Product Support Notices

VMware Cloud Director 10.1 does not support vSphere 7.0 and NSX-T Data Center 3.0. The interoperability certification is in progress and vSphere 7.0 and NSX-T Data Center 3.0 will be supported in a minor patch release of VMware Cloud Director 10.1.

External networks that are backed by VRF-lite tier-0 gateways in NSX-T Data Center are not supported.

End of Life and End of Support Warnings

- SQL Server database is no longer supported. Only the PostgreSQL database is supported.

- Oracle Linux is no longer supported as the host operating system to install the VMware Cloud Director
Edit document .
- VMware Cloud Director API version 20 and earlier are not supported.
- VMware Cloud Director API versions 27.0 - 29.0 are deprecated and are due to become unsupported after VMware Cloud Director 10.1
- VMware Cloud Director API version 30.0 is deprecated.
- The Flex-based UI has been removed from the product and is no longer supported.
- The `/api/sessions` API login endpoint was deprecated in VMware Cloud Director API version 33.0/VMware Cloud Director 10.0 and will be 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 and will be removed in a future release. You must use the `/api/server_status` for both HTTP and HTTPS protocols.
- The reset actions `/ldap/action/resetLdapCertificate` and `/ldap/action/resetLdapKeyStore` are removed from 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 will not be supported in future releases. 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 will not be supported in future vSphere and VMware Cloud Director releases.
- DSA and DSS certificates are no longer supported because no recommended cipher suites are available for them.

Upcoming End of Support Notice

- VMware Cloud Director API 34.0 (VMware Cloud Director 10.1) contains APIs that are under accelerated deprecation and will be removed in future releases. See VMware Cloud Director API Programming Guide.

Upgrading from Previous Releases

For more information on upgrading to VMware Cloud Director 10.1, 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 used by VMware Cloud Director 10.1, see VMware Ports and Protocols.

Compatibility Matrix

See the VMware Product Interoperability Matrixes for current information about:

Edit document

- VMware Cloud Director interoperability with other VMware platforms
- Supported VMware Cloud Director databases

Supported VMware Cloud Director Server Operating Systems

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

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 3.7.9 or 3.8.2

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

Supported Databases for Storing Historic Metric Data

You can configure your VMware Cloud Director installation to store metrics that VMware Cloud Director collects about virtual machine performance and resource consumption. Data for historic metrics is stored in a Cassandra database. VMware Cloud Director supports Cassandra versions 3.*x*.

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

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
c            pX11      procps
findutils    libXau    redhat-lsb
glibc        libXdmcp  sed
grep         libXext   tar
initscripts  libXi     wget
krb5-libs    libXt     which
libgcc       libXtst
```

Edit document

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 (disabled by default)
- TLS version 1.0 (disabled 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 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 *V* Edit document *irector 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
- Microsoft Internet Explorer 11

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

- **When you associate two VMware Cloud Director appliance sites, objects are not visible across the sites**
  If you make a site association and your sites have objects like organizations, organization VDCs, vApps, VMs, you cannot see the objects from the current site. The HTML 5 UI displays only the objects from the other associated site. The issue occurs during multisite fanout communication because the `/etc/hosts` file of the VMware Cloud Director appliance does not have correct contents.

- **Updating a VM sizing policy fails with a memory allocation error**
  If you convert an allocation-pool VDC to a flex organization VDC, vCloud Director keeps the maximum policy information from the allocation-pool VDC before the conversion. CPU or memory reservation guarantees higher than the reservations defined in the allocation-pool VDC fail with a `Virtual machine reservation or limit or shares settings are invalid` error.

- **Quiescing or pausing the primary cell in a multi-cell environment does not restart the periodical tasks on the secondary cell**
  In a multi-cell environment, when you quiesce or pause the primary cell, the periodical tasks that are running in the background of the primary cell are not started from the secondary cell.

- **Cloning a VM on a host-based storage policy with enabled data services to a VM with different host-based storage policy fails with an error**
  If you create a VM that is on a storage policy that has host-based rules like IOPS or VM Encryption enabled, trying to clone the VM and change the storage policy of the target VM fails with an

error `Changing or applying VM Storage Policies with Data Service capabilities during clone is disallowed. VM Storage Policies with Data Service capabilities can be assigned to the provisioned VM after the clone operation has been completed and before the VM has been powered on.`

Edit document

- **The global tenant role vApp Author can upload and create templates and media without having the necessary right for these operations**
  The global tenant role vApp Author by default has the `Add a vApp from My Cloud` right. Because this right and the `Template/Media: Create/Upload` right share a single operation, VMware Cloud Director incorrectly grants also the `Template/Media: Create/Upload` right to the vApp Author role.

  The issue is fixed. If you want the vApp Author role to continue to have the `Template/Media: Create/Upload` right, a service provider can add the right to the vApp Author Global Role and publish it to an organization.

- **Newly created virtual machines are deployed on the organization VDC default storage policy**
  In the vCloud Director Tenant Portal, when you create a new standalone virtual machine, the option to specify the storage policy is missing. As a result the created virtual machine is deployed with the default storage policy of the organization VDC.

Known Issues

- New **You cannot open a VM web console when using Microsoft Internet Explorer 11**
  Using Microsoft Internet Explorer 11 to connect to the console of a VM opens a white blank window and you cannot access the VM console.

  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 **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 **Using the VMware Cloud Director API to query a vApp returns empty fields for the numberOfCpus and MemoryAllocationMB attributes**

Edit document

When you use the VMware Cloud Director API 33.0 or an earlier version to run a vApp REST API query, API response body returns empty fields for the `numberOfCpus` and `MemoryAllocationMB` attributes. This can happen because the API schema does not include definition for the `numberOfCpus` and `MemoryAllocationMB` attributes.

Workaround: Use the VMware Cloud Director API 34.0 to query a vApp.

- **New 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".

  Workaround: Use the NSX-T Data Center policy API to update the redistribution configuration of the external network to which the NSX-T edge gateway is connected.

  1. Note the ID of the Tier-0 Router that backs the external network to which your NSX-T edge gateway is connected.
     - Perform a GET request to get a list of the tier-0 routers in your environment.
       `GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s`
     - Examine the list to identify the tier-0 by its display name, which matches the tier-0 router name in the General information tab for the external network in the VMware Cloud Director UI.

  2. `Update the external network (Tier-0 gateway) manually.`

     - Perform a GET request to obtain the list of `localeServices` on the router.
       `GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services`
       The response returns one locale service.
     - Copy the `localeService ID` and perform a GET request to examine it.

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

       The response returns a list of the properties for the locale service.

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

     - Modify the response as follows.

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

```
    ],
    ...
}
```

Edit document

  - Perform a PUT request with the modified properties to update the `localeService` of the Tier-0 router.

- New **Relocating a virtual machine to a different cluster fails if the target storage container is a datastore cluster**
  When you perform an operation that results in an attempt to relocate a virtual machine to a different cluster and the target storage container is a datastore cluster, the migration fails with a `NO_FEASIBLE_PLACEMENT_SOLUTION` error. In the VMware Cloud Director logs, you see a Storage DRS invocation error with `invalidProperty = spec.host`.

  Workaround:

  1. Use the vSphere Client to disable Storage DRS on the target datastore cluster or use the VMware Cloud Director API to change the target storage for the relocation to a datastore.

  2. Reattempt the failed operation.

- New **The VMware Cloud Director appliance deployment fails when you enable the setting to expire the root password upon the first login**
  If you attempt to deploy an appliance with enabled **Expire Root Password Upon First Login** setting, the deployment fails and the `/opt/vmware/var/log/firstboot` log file displays an error:

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

  Workaround: Disable the **Expire Root Password Upon First Login** setting and specify an initial root password that contains at least eight characters, one uppercase character, one lowercase character, one numeric digit, and one special character.

- New **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.

- New **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.

- New **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**

Edit document

In a multisite environment, while using the HTML5 UI, if you are logged in to a vCloud Director 10.0 site 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**.

- New **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.

- New **In a multisite mixed environment with VMware Cloud Director versions 10.0 and 10.1, trusting the certificates for vCenter Server and NSX connections works only for the objects from the local site**
  If you have a multisite environment with VMware Cloud Director versions 10.0 and 10.1 associated with each other, when you log in to one of the sites, you cannot register vCenter Server or NSX Manager instances on the other site.

  Workaround: Log into the site in which you want to register the vCenter Server or NSX Manager instance and start the registration process.

- New **In the VMware Cloud Director Tenant Portal, you cannot filter VMs by data center from the advanced filtering option for virtual machines under the Applications tab**
  In the VMware Cloud Director Tenant Portal, when you navigate to Virtual Machines under the Applications tab in the top navigation bar, filtering the virtual machines by data center from the advanced filtering option results in an error `Bad request: Unknown property name vdcName`.

  Workaround: From the top navigation bar, select **Data Centers** and select a data center to view the virtual machines in it.

- New **Extension services cannot process RabbitMQ messages from VMware Cloud Director**
  Extension services that rely on RabbitMQ cannot get the header `notification.type` from a message because the header has a new temporary name. The header name for VMware Cloud Director 10.1.0 is `notification.operationType`.

  Workaround: If your extension services process RabbitMQ messages from VMware Cloud Director and use the `notification.type` message header, you must change them. If the notification.type header is not available, extension services must get the value from the header `notification.operationType`. This change is needed only for version 10.1.0.

- **In the VMware Cloud Director Service Provider Admin Portal, deleting an organization virtual data center fails with an error**
  In the VMware Cloud Director Service Provider Admin Portal, if you add an edge gateway to your organization VDC and enable the gateway to provide VMware Cloud Director Distributed Routing, trying to delete the organization VDC recursively fails with a `Cannot delete organization VDC network` error message.

  Workaround:

Edit document

1. By using API, delete the organization VDC networks and the edge gateways associated with the nization VDC.
2. By using API, delete the organization VDC.

- **If you disable the provider access to the legacy API login endpoint, all API integrations that rely on the system administrator login stop working, including vCloud Usage Meter and vCloud Availability for VMware Cloud Director**
  Starting with vCloud Director 10.0, you can use separate VMware Cloud Director OpenAPI login endpoints for service provider and tenant access to VMware Cloud Director. If the service provider access to the legacy `/api/sessions` endpoint is disabled, it causes products that integrate with VMware Cloud Director, like vCloud Usage Meter and vCloud Availability for VMware Cloud Director, to stop working. These products will require a patch to continue to operate.

  The issue affects only system administrators. The tenant login is not affected.

  Workaround: Re-enable the service provider access to the legacy `/api/sessions` endpoint by using the cell management tool.

- **When you change the reservation guarantee values of a VDC, the existing VMs are not updated accordingly even after a reboot**
  If you have a flex organization VDC with the system default policy and powered-on virtual machines on that VDC are with the default sizing policy, when you increase the resource guarantee value of the VDC, the resource reservation for the existing VMs is not updated and they are also not marked as non-compliant. The issue occurs also when you convert a legacy VDC allocation model to a flex allocation model and the existing VMs become non-compliant with the new default policy of the flex organization VDC after the conversion.

  Workaround:

  1. To find the VM identifier, in the VMware Cloud Director Tenant Portal, navigate to the Details page of the VM. The URL shows the identifier `https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Identifier/general`
  2. To display the non-compliant VMs in the VMware Cloud Director UI, perform an explicit compliance check against the VMs by using the VMware Cloud Director API. `POST: https://VCD_IP_Address/api/vApp/vm-Identifier/action/checkComputePolicyCompliance`
  3. To reapply the policy and reconfigure the resource reservations, in the VMware Cloud Director Tenant Portal, click **Make VM Compliant** for a non-compliant VM.
- **VMware Cloud Director displays incorrect information about running VMs, total VMs, CPU and memory stats in dedicated vCenter Server instances**
  If a dedicated vCenter Server instance is version 6.0 Update 3i or earlier, 6.5 Update 2 or earlier, or 6.7 Update 1 or earlier, VMware Cloud Director displays incorrect information about running VMs, total VMs, and CPU and memory statistical information in the vCenter Server instance. The dedicated vCenter Server tile in the Tenant Portal and the dedicated vCenter Server information in the Service Provider Admin Portal display zero for both running VMs and total VMs, even when there are virtual machines in the vSphere environment.

  Workaround: Upgrade the vCenter Server instance to version 6.0 Update 3j, 6.5 Update 3, 6.7 Update 2, or later.

- **Changing the compute policy of a powered on VM might fail**
  When trying to change the compute policy of a powered on VM, if the new compute policy is associated with a provider VDC compute policy that has VM Groups or Logical VM Groups, an error occurs. The error message contains: `Underlying system error: com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation`.

  Workaround: Power off the VM, and retry the operation.

- **When using the VMware Cloud Director Service Provider Admin Portal with Firefox, you cannot** Edit document **nant 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.

- **VMware Cloud Director 10.1 supports only a list of input parameters of vRealize Orchestrator workflows**
  VMware Cloud Director 10.1 supports the following input parameters of vRealize Orchestrator workflows:

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

  Workaround: None

- **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.

- **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.