VMware vCenter Server 7.0 Update 2c Release Notes

vCenter Server 7.0 Update 2c | 24 AUG 2021 | ISO Build 18356314

Check for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in this Release
- Product Support Notices
- Resolved Issues
- Known Issues

What's New

- This release resolves CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22005, CVE-2021-22006, CVE-2021-22007, CVE-2021-22008, CVE-2021-22009, CVE-2021-22010, CVE-2021-22014, CVE-2021-22015, CVE-2021-22019, CVE-2021-22020. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2021-0020.

- For VMware vSphere with Kubernetes updates, see VMware vSphere with Kubernetes Release Notes.

- For Photon OS updates, see VMware vCenter Server Appliance Photon OS Security Patches.

Earlier Releases of vCenter Server 7.0

New features, resolved, and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes
- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1d Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server versions that support upgrade to vCenter Server Update 7.0 Update 2c, refer to VMware knowledge base article 67077.

Patches Contained in This Release

This release of vCenter Server 7.0 Update 2c delivers the following patch. See the VMware Patch Download Center for more information on downloading patches.

- Patch for VMware vCenter Server 7.0 Update 2c

Patch for VMware vCenter Server 7.0 Update 2c

Product Patch for vCenter Server containing VMware software fixes, security fixes, and third-party product fixes.

This patch is applicable to vCenter Server.

Download Filename	VMware-vCenter-Server-Appliance-7.0.2.00400-18356314-patch-FP.iso
Build	18356314
Download Size	5550.2 MB
md5sum	31bbecb2bac8d42d7d962a2e8ce1c46e
sha1checksum	a77c8831258696d5cb731737003e63b7ab4b28db

Download and Installation

You can download this patch by going to the VMware Patch Download Center and selecting **VC** from the **Select a Product** drop-down menu.

1. Attach the `VMware-vCenter-Server-Appliance-7.0.2.00400-18356314-patch-FP.iso` file to the vCenter Server CD or DVD drive.
2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:

- To stage the ISO:

  `software-packages stage --iso`
  - To see the staged content:

  `software-packages list --staged`
  - To install the staged rpms:

  `software-packages install --staged`

For more information on using the vCenter Server shells, see VMware knowledge base article [2100508](#).

For more information on patching vCenter Server, see [Patching the vCenter Server Appliance](#).

For more information on staging patches, see [Stage Patches to vCenter Server Appliance](#).

For more information on installing patches, see [Install vCenter Server Appliance Patches](#).

For more information on patching using the Appliance Management Interface, see [Patching the vCenter Server by Using the Appliance Management Interface](#).

Product Support Notices

- **Discontinuation of Trusted Platform Module (TPM) 1.2 in a future major vSphere release:** VMware intends in a future major vSphere release to discontinue support of TPM 1.2 and associated features such as TPM 1.2 with TXT. To get full use of vSphere features, you can use TPM 2.0 instead of TPM 1.2. Support for TPM 1.2 continues in all vSphere 7.0.x releases, updates, and patches. However, you will not see a deprecation warning for TPM 1.2 during installation or updates of 7.0.x releases.

- **Your vCenter Server system must reboot after an update to vCenter Server 7.0 Update 2c**: After updating your vCenter Server system to version vCenter Server 7.0 Update 2c from a previous version of vCenter Server 7.0.x, a reboot is required to ensure critical kernel patches are applied. You must manually restart vCenter Server.

Resolved Issues

The resolved issues are grouped as follows.

- [Storage Issues](#)
- [Security Issues](#)
- [vSAN Issues](#)
- [vCenter Server and vSphere Client Issues](#)
- [Installation, Upgrade and Migration Issues](#)
- [Auto Deploy Issues](#)
- [Miscellaneous Issues](#)
- [vSphere Lifecycle Manager Issues](#)
- [Guest OS Issues](#)
- [Virtual Machine Management Issues](#)
- [Networking Issues](#)
- [vCenter Server High Availability Issues](#)

Storage Issues

- **NEW:** If you have ESXi hosts of version 6.5.x in a vCenter Server system of version 7.0 Update 2 and later, some vSphere Web Services API calls might not work on such hosts
  Some managed objects in ESXi 6.5.x, such as `vim.vslm.vcenter.VStorageObjectManager`, define the `apiVersion` by only 2 digits separated by a single dot, such as `<a>.<b>`. However, starting from vCenter Server 7.0 Update 2, for some tasks, such as `deleteVStorage_task`, the `apiVersion` must be defined by a minimum of 3 digits. For example `<a>.<b>.<c>` or `<a>.<b>.<c>.<d>`. As a result, when you use the `deleteVStorage_task` method on an ESXi host of version 6.5.x in a vCenter Server system of version 7.0 Update 2 and later, it does not complete successfully. If you use a Java client, you see an error such as `A specified parameter was not correct: version`.

  This issue is resolved in this release.

- **You cannot register Dell EMC Unity 500 or 600 vSphere API for Storage Awareness (VASA) provider to a vCenter Server system**
  Attempts to register a Dell EMC Unity 500 or 600 VASA provider to a vCenter Server system from **Configure** > **Security** > **Storage Providers** persistently fail with an error. In the vSphere Client, you see the message `A problem was encountered while provisioning a VMware Certificate Authority (VMCA) signed certificate for the provider.` The issue occurs in both fresh installations and upgraded environments.

  This issue is resolved in this release.

- **vCenter Server upgrades fail, because in the GUI installer you do not see the option to change the export directory to a larger partition**
  In stage 2 of the vCenter Server upgrade, you do not see the option to change the export directory to a larger partition from the default. As a result, upgrade of the vCenter Server fails. In the GUI installer, you see an error such as `Insufficient space on the source export partition '/'`.

  This issue is resolved in this release. The Export directory option is available.

Security Issues
- **Updates to OpenSSL library**

The OpenSSL-1.1.1 library is updated to version 1.1.1k.

The OpenSSL-1.0.2 library is updated to version 1.0.2y.

- **Update to cURL**

  cURL is updated to version 7.74.0.

- **Update to JRE**

  Oracle (Sun) JRE is updated to version 8.0.291.

- **Update to the Python libraries**

  The Python 3.7 library is updated to version 3.7.10.

- **Update to the Spring Framework**

  The Spring Framework is updated to version 5.2.13.

- **Update to the Apache Tomcat server**

  The Apache Tomcat server is updated to version 8.5.63.

- **Responses from a remote web server on port 9087 might not have an HTTP Strict Transport Security (HSTS) response header**

  Responses from a remote web server on port 9087 might lack an HSTS response header and allow unencrypted connections.

  This issue is resolved in this release.

- **Upgrade of Eclipse Jetty**

  Eclipse Jetty is upgraded to version 9.4.39.

vSAN Issues

- **You see incorrect scheduled time for resynchronization tasks in a vSAN cluster**

  In a vSAN cluster, when you navigate to **Monitor** > **vSAN** > **Resyncing Objects** to see the status of ongoing, scheduled or pending resynchronization tasks, the **Scheduled resyncing** time might be in the past. The issue occurs only when the **Object repair timer** value is set to a big number, 36000 minutes and more, as compared to the default 60 min.

  This issue is resolved in this release.

- **vCenter Server services might fail due to full log directory**

  In rare cases, if the `vmware-vsan-health-service.log` fails to rotate, vCenter Server services might fail when the log directory becomes full.

  This issue is resolved in this release.

vCenter Server and vSphere Client Issues

- **You see only CPU, Memory and Hard disks in the Edit Settings dialog box of some virtual machines**

  When a virtual machine has 6 or more hard disks, the Hard disks section in the Edit Settings dialog box takes most of the screen. As a result, you have the impression that the Edit Settings dialog box displays only CPU, Memory and Hard disks from the virtual machine settings. All settings are available if you scroll down in the dialog box.

  This issue is resolved in this release.

Installation, Upgrade and Migration Issues

- **You cannot log in to your vCenter Server system after a multi-step upgrade to vCenter Server 7.0 Update 2**

  If you perform a multi-step upgrade of your vCenter Server system with an external Platform Services Controller from 5.5 to 6.0 to 6.5 to 6.7 to 7.0 Update 2, the original trusted roots might be missing from the VMware Endpoint Certificate Store (VECS) and tokens issued by the Security Token Service (STS) appear as invalid. As a result, you cannot log in to the vCenter Center system after the upgrade. In the vSphere Client, you see a message similar to `[500] An error occurred while fetching identity providers. Try again`.

  This issue is resolved in this release.

- **You see an unexpected error message in Update Planner**

  If the PNID of the management network of your vCenter Server system contains lower and upper case characters, the Update Planner fails to fetch updates and generate interoperability reports. In the vSphere Client, you see an error such as `Unexpected error occurred while fetching the updates`.

  This issue is resolved in this release.

Auto Deploy Issues

- **Due to a caching issue, ESXi hosts might fail to boot from Auto Deploy after an upgrade to vCenter Server 7.0 and later**

  After you upgrade your system to vCenter Server 7.0 and later, stale cache data might cause Auto Deploy to stop provisioning ESXi hosts. The hosts fail with an error such as `Could not boot: HTTP 5xx Server Error`.

  This issue is resolved in this release.

Miscellaneous Issues

- **NEW**: **You see vCenter Server event reports that Trusted Hosts attestation status is unset on every 5 minutes**

  In the vSphere Client **Events** tab, you see reports that Trusted Hosts attestation status is unset on every 5 minutes.

Messages are similar to:

```
Description: dd/mm/yyyy, hh:mm:ss
Trusted Host attestation status unset.
Type: Information
Target: Event
Type ID: com.vmware.vc.TaHostAttestUnsetEven
```

- **A ConfigTarget call delays virtual machine response time**
  A `ConfigTarget` call that determines VM configuration choices regarding available ESXi host resources might cause a delay in acquiring disk information from the host. As a result, you might see a delay in virtual machine response time. For example, opening the Edit Settings of a VM takes unusually long.

  This issue is resolved in this release. The fix optimizes `ConfigTarget` VMODL API requests.

- **You do not see historical data in Performance Charts in the vSphere Client**
  You see real-time data, but no historical data for the past day, week or month in the Performance Charts in the vSphere Client. The stats data is present in the vCenter Server database, but not displayed.

  This issue is resolved in this release.

- **The Host view of vCenter Server performance charts displays a no data error**
  In the vSphere Client, when you navigate to the Host view of vCenter Server performance charts, you see an error such as `no performance data is available for the currently selected metrics` in the Memory Usage, Disk (KBps), Disk (Number), and CPU Usage charts. The issue occurs after an upgrade to vCenter Server 7.0 Update 1.

  This issue is resolved in this release.

vSphere Lifecycle Manager Issues

- **vSphere Lifecycle Manager cluster image scan fails with a VIB relation error when the image contains the Intel-icen Component**
  If you add the Intel-icen Component to a vSphere Lifecycle Manager image by using a vendor add-on or as a standalone Component, vSphere Lifecycle Manager might not handle the custom Component properly as a replacement of the icen Component in the base image. In the vSphere Client, you see an error such as `Component metadata error or VIB relation error`.
  In the `imageservice.log`, you see logs such as:
  `ERROR Generating effective image failed: Final validation failed with these errors: "["File path of '/usr/lib/vmware/vmkmod/icen' is claimed by multiple non-overlay VIBs: {'VMW_bootbank_icen_', 'INT_bootbank_icen_'}", "File path of '/usr/share/hwdata/default.pciids.d/icen.ids' is claimed by multiple non-overlay VIBs: ...`.

  This issue is resolved in this release.

- **vCenter Server 7.0 Update 2 does not support No Proxy settings**
  No Proxy configurations of hardware support manager plug-ins or local depot servers do not work on vCenter Server 7.0 Update 2.

  This issue is resolved in this release.

Guest OS Issues

- **You see low-memory warnings for vCenter Server even when the system is not busy**
  A kernel memory accounting issue might cause vCenter Server to consume more memory than usual, even when the system is not busy. In the vCenter Server Appliance Management Interface (VAMI) you see a warning such as `Appliance is running low on Memory. Add more memory to the machine`.

  This issue is resolved in this release.

Virtual Machine Management Issues

- **If host encryption mode does not automatically switch on, all encrypted VMs in the host might be in a locked state**
  In rare occasions, host encryption mode might not be automatically enabled when vSphere Native Key Provider or a trusted key provider register virtual machines for encryption. For example, after you complete a test recovery of your system by using the Site Recovery Manager. As a result, all encrypted VMs in the host might be in a locked state.

  This issue is resolved in this release.

- **After a vCenter Server or ESXi host reboot, all encrypted VMs in the host might be in a locked state**
  In rare cases, vCenter Server might lose track of virtual machine keys reference records on an ESXi host. As a result, after a restart of the vCenter Server or the host, all encrypted virtual machines in that host are in a locked state.

  This issue is resolved in this release. The fix makes sure that vCenter Server never clears VM key reference records in the vCenter Server database, even if host encryption fails.

Networking Issues

- **When you create a distributed port group, you do not see any ESXi hosts in the ESXi hosts list**
  After you add a distributed port group to a vSphere Distributed Switch, you might not see any ESXi hosts in the ESXi hosts list, although you have hosts connected to the VDS.

This issue is resolved in this release.

vCenter Server High Availability Issues

- **If the Active Directory domain in your vCenter Single Sign-On is an external identity source, vCenter Server High Availability deployment might fail**
  If the Active Directory domain in your vCenter Single Sign-On is an external identity source, vCenter Server High Availability deployment might fail with an error that PostgreSQL server is not configured correctly.

  This issue is resolved in this release.

- **VM Component Protection (VMCP) does not respond to All Paths Down (APD) events**
  If you have VMCP enabled in your vSphere environment, a rare issue with the vSphere High Availability management agent on ESXi hosts, FDM, might prevent response to APD events. As a result, affected virtual machines do not restart on another host.

  In the `/var/log/vobd.log` file you see messages such as:

  `2021-03-11T09:49:57.123Z: [APDCorrelator] 460296002450us: [vob.storage.apd.timeout] Device or filesystem with identifier [naa.600601607b477826e60ef95ed62e643f]` `has entered the All Paths Down Timeout state after being in the All Paths Down state for 140 seconds. I/Os will now be fast failed.`

  In the `/var/log/fdm.log` file, you see messages such as:

  `2021-03-11T09:49:57.754Z warning fdm[2104475] [Originator@6876 sub=Election opID=SWI-3ab50c2a] IM reprts no locally accessible datastores`

  This issue is resolved in this release.

Known Issues

The known issues are grouped as follows.

- [Installation, Upgrade and Migration Issues](#)
- [vSphere Lifecycle Manager Issues](#)
- [vCenter Server and vSphere Client Issues](#)
- [Known Issues from Prior Releases](#)

Installation, Upgrade and Migration Issues

- **ESXi upgrade from 7.0.x to a later version on a 7.0 vCenter Server system fails**
  On a vCenter Server system of version 7.0, if you attempt to update ESXi hosts of version 7.0.x to a later version, for example 7.0 Update 1 to 7.0 Update 2a, by using an vSphere Lifecycle Manager upgrade baseline, the upgrade fails. In the vSphere Client, you see an error such as `Upgrade is not supported for host`.

  Workaround: You must first upgrade your vCenter Server to the required 7.0.x version and then upgrade ESXi hosts by using a vSphere Lifecycle Manager upgrade baseline. Alternatively, use an interactive upgrade from a CD, DVD or USB, a scripted upgrade, or ESXCLI instead of a vSphere Lifecycle Manager upgrade baseline.

- **Upgrade to vCenter Server 7.0 Update 2 by using the GUI installer stops at 50%**
  Upgrade to vCenter Server 7.0 Update 2 by using the GUI installer stops at 50%. In stage 2 of the deployment, you see an error message such as `Unable to authenticate user`.

  Workaround: Use `https://appliance-IP-address-or-FQDN:5480` in a Web browser to complete the installation.

vSphere Lifecycle Manager Issues

- **When you try to check VMware Tools or VM Hardware compliance status, you see a status 500 error and the check returns no results**
  In the vSphere Client, when you navigate to the **Updates** tab of a container object: host, cluster, data center, or vCenter Server instance, to check VMware Tools or VM Hardware compliance status, you might see a status 500 error. The check works only if you navigate to the **Updates** tab of a virtual machine.

  Workaround: None

vCenter Server and vSphere Client Issues

- **You cannot migrate vSphere Cluster Services (vCLS) agent virtual machines and see a no privileges error**
  vSphere admins might not automatically get Containerized Permissions that protect vCLS VMs. As a result, although you have admin permissions, you might not be able to migrate vCLS VMs. In the vSphere Client, you see an error such as:
  `You have no privileges to view vCLS (1) object`

  Workaround: Log out of the vSphere Client and then log in as admin.

Known Issues from Prior Releases

To view a list of previous known issues, click [here](#).

Copyright © Broadcom