VMware vCenter Server 8.0 Update 2d Release Notes

VMware vSphere 8.0

vmware by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Introduction

1

VMware vCenter Server 8.0 Update 2d | 17 JUN 2024 | ISO Build 23929136

Check for additions and updates to these release notes.

What's New

2

- This release resolves CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0012.

Earlier Releases of vCenter Server 8.0

3

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 8.0 are:

- VMware vCenter Server 8.0 Update 2c Release Notes
- VMware vCenter Server 8.0 Update 2b Release Notes
- VMware vCenter Server 8.0 Update 1d Release Notes
- VMware vCenter Server 8.0 Update 2a Release Notes
- VMware vCenter Server 8.0 Update 2 Release Notes
- VMware vCenter Server 8.0 Update 1c Release Notes
- VMware vCenter Server 8.0 Update 1b Release Notes
- VMware vCenter Server 8.0 Update 1a Release Notes
- VMware vCenter Server 8.0 Update 1 Release Notes
- VMware vCenter Server 8.0c Release Notes
- VMware vCenter Server 8.0b Release Notes
- VMware vCenter Server 8.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 8.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release 4

Read the following topics next:

- Patch for VMware vCenter Server 8.0 Update 2d
- Download and Installation

Patch for VMware vCenter Server 8.0 Update 2d

Product Patch for vCenter Server containing VMware software fixes.

This patch is applicable to vCenter Server.

Download Filename	VMware-vCenter-Server-Appliance-8.0.2.00400-23929136-patch-FP.iso
Build	23929136
Download Size	7874.2 MB
sha256checksum	566d3a9b866ce7af27c0655ae2a7115fc76ca226f1917aa26d4890175243b2e0
PRs fixed	NA
CVEs	CVE-2024-37079, CVE-2024-37080, CVE-2024-37081

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

1 Attach the `VMware-vCenter-Server-Appliance-8.0.2.00400-23929136-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 and Updating vCenter Server 8.0 Deployments.

For more information on staging patches, see Upgrading the vCenter Server Appliance.

Resolved Issues

5

Read the following topics next:

- Security Issues

Security Issues

- This release resolves CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0012.

Known Issues from Previous Releases

6

Read the following topics next:

- Installation, Upgrade, and Migration Issues
- Miscellaneous Issues
- Networking Issues
- Storage Issues
- vCenter Server and vSphere Client Issues
- Virtual Machine Management Issues
- vSphere Lifecycle Manager Issues
- VMware Host Client Issues
- Security Features Issues

Installation, Upgrade, and Migration Issues

- **You see a security warning for the ESX Agent Manager configuration during the pre-check phase of a vCenter upgrade**

  During the pre-check phase of a vCenter update or upgrade, in the vSphere Client and logs, you might see an error such as:

  ```
  Source ESX Agent Manager Configuration contains URLs that are not trusted by the System! Please refer to https://kb.vmware.com/s/article/93526 to trust the URLs: <LIST_OF_URLs>
  ```

  Or

  ```
  Source vSphere ESX Agent Manager (EAM) upgrade failed to obtain EAM URLs to check against trusted certificates by the System! Verify that the ESX Agent Manager extension is running properly on the source vCenter Server instance and https://VC_IP/eam/mob presents correct data. If log in to the MOB is not successful, try resolving the issue with https://kb.vmware.com/s/article/94934.
  ```

  Workaround: For more information, see VMware knowledge base articles 93526 and 94934.

- **In a mixed vSphere 7.x and 8.x environment with vSphere DRS, an incompatible virtual machine might prevent an ESXi host to enter maintenance mode**

  In a mixed vSphere 7.x and 8.x environment with DRS, a VM of 7.x version that is not compatible with ESXi 8.0 Update 1 and later might prevent an ESXi 8.0 Update 1 host to enter maintenance mode. The issue is specific for virtual machines with VMDK on a vSphere Virtual Volumes datastore. In the vSphere Client, you see an error such as **Waiting for all VMs to be powered off or suspended or migrated. In a DRS cluster check the Faults page on the DRS tab for troubleshooting.**

  Workaround: Power-off the incompatible virtual machine.

- **You see an error Failed to get ceip status in the Virtual Appliance Management Interface (VAMI) during update to vCenter Server 8.0 Update 1**

  During an update, vCenter stops and restarts the VMDir service and within this interval, if you try to log in to the VAMI, you might see an error such as **Failed to get ceip status**. This is expected and does not indicate an actual issue with the vCenter system.

  Workaround: Wait for the VMDir service to restart and refresh the Virtual Appliance Management Interface.

- **vCenter upgrade or update to 8.0 Update 2a or later fails during precheck with the error "VMCA root certificate validation failed"**

  If your vCenter system has a legacy VMCA root certificate dating back to version 5.x which does not have the Subject Key Identifier (SKID) extension, upgrades and updates to vCenter 8.0 Update 2 and later fail because the OpenSSL version 3.0 in 8.0 Update 2 is not compatible with legacy root certificates. vCenter Server 8.0 Update 2a adds a precheck to detect this issue and shows the error message **VMCA root certificate validation failed** if the source vCenter has VMCA root certificate without SKID.

  Workaround: Regenerate a VMCA root certificate by following the steps in VMware knowledge base article 94840.

- **A reduced downtime upgrade (RDU) on a vCenter system might fail when you use Update Planner**

  During RDU, if you use Update Planner, in the vSphere Client you might see an error such as: `Update 8.0.2.00000 for component vlcm is not found.`

  Workaround: For more information, see VMware knowledge base articles 94779 and 92659.

- **Failed parallel remediation by using vSphere Lifecycle Manager on one ESXi host might cause other hosts to remain in a pending reboot state**

  An accidental loss of network connectivity during a parallel remediation by using vSphere Lifecycle Manager might cause the operation to fail on one of the ESXi hosts. Remediation on other hosts continues, but the hosts cannot reboot to complete the task.

  Workaround: If an ESXi host consistently fails remediation attempts, manually trigger a reboot. For more information, see VMware knowledge base article 91260.

- **You see a security warning for the ESX Agent Manager configuration during the pre-check phase of a vCenter upgrade**

  During the pre-check phase of a vCenter update or upgrade, in the vSphere Client and logs, you might see an error such as:

  ```
  Source ESX Agent Manager Configuration contains URLs that are not trusted by the System! Verify following URLs and their respective statuses and follow KB 93526.
  ```

  Workaround: For more information, see VMware knowledge base article 93526.

- **Firmware compliance details are missing from a vSphere Lifecycle Manager image compliance report for an ESXi standalone host**

  Firmware compliance details might be missing from a vSphere Lifecycle Manager image compliance report for an ESXi standalone host in two cases:

  a You run a compliance report against a standalone host managed with a vSphere Lifecycle Manager image from vSphere Client and then navigate away before the compliance report gets generated.

  b You trigger a page refresh after the image compliance reports are generated.

  In such cases, even when you have the firmware package available in the Desired State, the firmware compliance section remains empty when you revisit or refresh the vSphere Client browsing session. If you use GET image compliance API, then firmware compliance details are missing from the response.

  Workaround: Invoke the image compliance scan for a standalone host managed with a vSphere Lifecycle Manager image by using the vSphere Client and do not navigate away or refresh the browser. For API, use the Check image compliance API for fetching the firmware details as apposed to GET image compliance.

- **You see vCenter update status as failed although it completes successfully**

  A rare race condition might cause vCenter to report a successful update as failed. The issue occurs if during vCenter reboot `/storage/core` unmounts before the system acknowledges the **Installation complete** status. As a result, the update fails with an error such as `No such file or directory: '/storage/core/software-update/install_operation'`. In the `software-packages.logs`, you see errors such as:

  ```
  2023-08-17T10:57:59.229 [15033]DEBUG:vmware.appliance.update.update_state:In State._get using state file /etc/applmgmt/appliance/software_update_state.conf

  2023-08-17T10:57:59.229 [15033]INFO:vmware.appliance.update.update_state:Found operation in progress /storage/core/software-update/install_operation

  2023-08-17T10:57:59.229 [15033]ERROR:vmware.appliance.update.update_functions:Can't read JSON file /storage/core/software-update/install_operation [Errno 2] No such file or directory: '/storage/core/software-update/install_operation'
  ```

```
2023-08-17T10:57:59.229 [15033]DEBUG:vmware.appliance.update.update_state:Operation
in progress is orphaned

2023-08-17T10:57:59.229 [15033]DEBUG:vmware.appliance.update.update_state:Operation
in progress is finished

2023-08-17T10:57:59.229 [15033]DEBUG:vmware.appliance.update.update_state:Writing
to state file from State._get

2023-08-17T10:57:59.229 [15033]DEBUG:vmware.appliance.update.update_state:In
State._writeInfo writing to state file /etc/applmgmt/appliance/
software_update_state.conf

2023-08-17T10:57:59.229 [15033]INFO:vmware.vherd.base.software_update:Installation
failed. Please collect the VC support bundle.
```

Workaround: Check if vCenter restarts successfully and the vCenter health status is green, and ignore the failure report.

- **Patching to vCenter 8.0 Update 2 fails in IPv6 environments with no DNS server and hostname**

  When you update your vCenter system to 8.0 Update 2 from an earlier version of 8.x, if your system uses an IPv6 network without a hostname, such as PNID, and a DNS server, in the VMware Appliance Management Interface you might see an error such as `Data conversion/ Post install hook failed`.

  Workaround: Manually update the `/etc/hosts` file with the missing IPv6 loopback entry: `::1 localhost ipv6-localhost ipv6-loopback` and reboot the system.

  See this example:

  ```
  root@localhost []# cat /etc/hosts
  ```

  `# Begin /etc/hosts` (network card version)

  ```
  127.0.0.1 localhost.localdomain

  127.0.0.1 localhost

  ::1 localhost ipv6-localhost ipv6-loopback
  ```

- **If you apply a host profile using a software FCoE configuration to an ESXi 8.0 host, the operation fails with a validation error**

  Starting from vSphere 7.0, software FCoE is deprecated, and in vSphere 8.0 software FCoE profiles are not supported. If you try to apply a host profile from an earlier version to an ESXi 8.0 host, for example to edit the host customization, the operation fails. In the vSphere Client, you see an error such as `Host Customizations validation error`.

  Workaround: Disable the Software FCoE Configuration subprofile in the host profile.

- **During a reduced downtime upgrade (RDU), when configuring Target VM network settings, you see no network portgroups**

In very rare cases, during a reduced downtime upgrade of a single self-managed vCenter instance that uses a migration-based method, when a source vCenter VM has thin disk provisioning and the target vCenter cluster does not have enough storage to accommodate the required space for the default thick disk mode selected by the validation process, you might see no network portgroups in the **Target VM deployment** wizard. In the vSphere Client, if you select **Same Configuration** in the **Deployment type** step of the **Target VM deployment** wizard, you see an empty error message in the **Network Settings** screen and no portgroups available.

Workaround: In the **Deployment type** step of the **Target VM deployment** wizard, select **Detailed Configuration**.

- **You cannot use ESXi hosts of version 8.0 as a reference host for existing host profiles of earlier ESXi versions**

  Validation of existing host profiles for ESXi versions 7.x, 6.7.x and 6.5.x fails when only an 8.0 reference host is available in the inventory.

  Workaround: Make sure you have a reference host of the respective version in the inventory. For example, use an ESXi 7.0 Update 2 reference host to update or edit an ESXi 7.0 Update 2 host profile.

- **URL-based patching or file-based backup of vCenter 8.0 Update 2 might fail due to OpenSSL noncompliance to Federal Information Processing Standards (FIPS)**

  With vCenter 8.0 Update 2, OpenSSL works only with Diffie-Hellman parameters compliant to NIST SP 800-56A and FIPS 140-2. For URL-based patching or file-based backup of vCenter 8.0 Update 2 systems, FTPS servers in your environment must support the following ciphers:

OpenSSL Cipher Suite	Name AT-TLS Cipher Suite Name	Hexadecimal Value
DHE-RSA-AES256-SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	39
DHE-DSS-AES256-SHA	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	38
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA	35
EDH-RSA-DES-CBC3-SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	16
EDH-DSS-DES-CBC3-SHA	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	13
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA	0A
DHE-RSA-AES128-SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	33
DHE-DSS-AES128-SHA	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	32
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA	2F

  Workaround: Make sure your file servers are FIPS compliant.

- **VMNICs might be down after an upgrade to ESXi 8.0**

If the peer physical switch of a VMNIC does not support Media Auto Detect, or Media Auto Detect is disabled, and the VMNIC link is set down and then up, the link remains down after upgrade to or installation of ESXi 8.0.

Workaround: Use either of these 2 options:

a Enable the option `media-auto-detect` in the BIOS settings by navigating to System Setup Main Menu, usually by pressing **F2** or opening a virtual console, and then **Device Settings** > *<specific broadcom NIC>* > **Device Configuration Menu** > **Media Auto Detect**. Reboot the host.

b Alternatively, use an ESXCLI command similar to: `esxcli network nic set -S <your speed> -D full -n <your nic>`. With this option, you also set a fixed speed to the link, and it does not require a reboot.

- **After upgrade to ESXi 8.0, you might lose some nmlx5_core driver module settings due to obsolete parameters**

  Some module parameters for the `nmlx5_core` driver, such as `device_rss`, `drss` and `rss`, are deprecated in ESXi 8.0 and any custom values, different from the default values, are not kept after an upgrade to ESXi 8.0.

  Workaround: Replace the values of the `device_rss`, `drss` and `rss` parameters as follows:

  - `device_rss`: Use the `DRSS` parameter.
  - `drss`: Use the `DRSS` parameter.
  - `rss`: Use the `RSS` parameter.

- **Second stage of vCenter Server restore procedure freezes at 90%**

  When you use the vCenter Server GUI installer or the vCenter Server Appliance Management Interface (VAMI) to restore a vCenter from a file-based backup, the restore workflow might freeze at 90% with an error `401 Unable to authenticate user`, even though the task completes successfully in the backend. The issue occurs if the deployed machine has a different time than the NTP server, which requires a time sync. As a result of the time sync, clock skew might fail the running session of the GUI or VAMI.

  Workaround: If you use the GUI installer, you can get the restore status by using the `restore.job.get` command from the `appliancesh` shell. If you use VAMI, refresh your browser.

Miscellaneous Issues

- **In Hybrid Linked Mode, the cloud vCenter is not able to discover plug-ins deployed on an on-prem vCenter**

Hybrid Linked Mode allows you to link your cloud vCenter Server instance with an on-premises vCenter Single Sign-On domain, but the cloud vCenter might not be able to discover plug-ins deployed on the on-prem instance because it does not have the necessary permissions.

Workaround: Install the vCenter Cloud Gateway in your on-premises environment and either browse the plug-ins deployed on the on-prem instance from the VMware Cloud Console or directly from the vSphere Client on the on-prem vCenter.

- **You see incorrect Maximum Size value for thin-provisioned virtual disks**

  In the vSphere Client, when you look at the settings of a VM with a thin-provisioned virtual disk, you might see the **Maximum Size** value for the disk larger than the capacity of the datastore where the disk is located. For example, if a datastore capacity is 100GB of which 90GB are available, and a thin-provisioned virtual disk has 50GB capacity, of which only 10GB are utilized, you might see a **Maximum Size** value of 140 GB, adding the available datastore capacity to the overall disk capacity, not its actual utilization.

  Workaround: None

- **In a vCenter Server system with DPUs, if IPv6 is disabled, you cannot manage DPUs**

  Although the vSphere Client allows the operation, if you disable IPv6 on an ESXi host with DPUs, you cannot use the DPUs, because the internal communication between the host and the devices depends on IPv6. The issue affects only ESXi hosts with DPUs.

  Workaround: Make sure IPv6 is enabled on ESXi hosts with DPUs.

- **You cannot customize firewall rule configuration with the option 'Only allow connections from the following networks' on ESXi hosts**

  Starting with vSphere 8.0 Update 2, you cannot customize firewall rule configuration with the option **Only allow connections from the following networks** on ESXi hosts. For example, in the VMware Host Client, when you navigate to **Networking > Firewall rules**, select **DHCP client**, provide an IP and check **Only allow connections from the following networks**, the operation fails with an error such as `Operation failed, diagnostics report: Invalid operation requested: Can not change allowed ip list this ruleset, it is owned by system service.`. This is expected behavior.

  Workaround: None

- **You might see 10 min delay in rebooting an ESXi host on HPE server with pre-installed Pensando DPU**

  In rare cases, HPE servers with pre-installed Pensando DPU might take more than 10 minutes to reboot in case of a failure of the DPU. As a result, ESXi hosts might fail with a purple diagnostic screen and the default wait time is 10 minutes.

  Workaround: None.

- **If you have an USB interface enabled in a remote management application that you use to install ESXi 8.0, you see an additional standard switch vSwitchBMC with uplink vusb0**

Starting with vSphere 8.0, in both Integrated Dell Remote Access Controller (iDRAC) and HP Integrated Lights Out (ILO), when you have an USB interface enabled, vUSB or vNIC respectively, an additional standard switch `vSwitchBMC` with uplink `vusb0` gets created on the ESXi host. This is expected, in view of the introduction of data processing units (DPUs) on some servers but might cause the VMware Cloud Foundation Bring-Up process to fail.

Workaround: Before vSphere 8.0 installation, disable the USB interface in the remote management application that you use by following vendor documentation.

After vSphere 8.0 installation, use the ESXCLI command `esxcfg-advcfg -s 0 /Net/BMCNetworkEnable` to prevent the creation of a virtual switch `vSwitchBMC` and associated portgroups on the next reboot of host.

See this script as an example:

```
~# esxcfg-advcfg -s 0 /Net/BMCNetworkEnable
```

The value of BMCNetworkEnable is 0 and the service is disabled.

```
~# reboot
```

On host reboot, no virtual switch, PortGroup and VMKNIC are created in the host related to remote management application network.

- **If an NVIDIA BlueField DPU is in hardware offload mode disabled, virtual machines with configured SR-IOV virtual function cannot power on**

  NVIDIA BlueField DPUs must be in hardware offload mode enabled to allow virtual machines with configured SR-IOV virtual function to power on and operate.

  Workaround: Always use the default hardware offload mode enabled for NVIDIA BlueField DPUs when you have VMs with configured SR-IOV virtual function connected to a virtual switch.

- **In the Virtual Appliance Management Interface (VAMI), you see a warning message during the pre-upgrade stage**

  Moving vSphere plug-ins to a remote plug-in architecture, vSphere 8.0 deprecates support for local plug-ins. If your 8.0 vSphere environment has local plug-ins, some breaking changes for such plug-ins might cause the pre-upgrade check by using VAMI to fail.

  In the Pre-Update Check Results screen, you see an error such as:

  ```
  Warning message: The compatibility of plug-in package(s) %s with the new vCenter Server version cannot be validated. They may not function properly after vCenter Server upgrade.

  Resolution: Please contact the plug-in vendor and make sure the package is compatible with the new vCenter Server version.
  ```

Workaround: Refer to the VMware Compatibility Guide and VMware Product Interoperability Matrix or contact the plug-in vendors for recommendations to make sure local plug-ins in your environment are compatible with vCenter Server 8.0 before you continue with the upgrade. For more information, see the blog Deprecating the Local Plugins :- The Next Step in vSphere Client Extensibility Evolution and VMware knowledge base article 87880.

- **You cannot remove a PCI passthrough device assigned to a virtual Non-Uniform Memory Access (NUMA) node from a virtual machine with CPU Hot Add enabled**

  Although by default when you enable CPU Hot Add to allow the addition of vCPUs to a running virtual machine, virtual NUMA topology is deactivated, if you have a PCI passthrough device assigned to a NUMA node, attempts to remove the device end with an error. In the vSphere Client, you see messages such as `Invalid virtual machine configuration. Virtual NUMA cannot be configured when CPU hotadd is enabled`.

  Workaround: See VMware knowledge base article 89638.

Networking Issues

- **Overlapping hot-add and hot-remove operations for DirectPath I/O devices might fail**

  With vSphere 8.0 Update 1, by using vSphere API you can add or remove a DirectPath I/O device without powering off VMs. However, if you run several operations at the same time, some of the overlapping tasks might fail.

  Workaround: Plan for 20 seconds processing time between each hot-add or hot-remove operation for DirectPath I/O devices.

- **Hot adding and removing of DirectPath I/O devices is not automatically enabled on virtual machines**

  With vSphere 8.0 Update 1, by using vSphere API you can add or remove a DirectPath I/O device without powering off VMs. When you enable the hotplug functionality that allows you to hot add and remove DirectPath I/O devices to a VM, if you use such a VM to create an OVF and deploy a new VM, the new VM might not have the hotplug functionality automatically enabled.

  Workaround: Enable the hotplug functionality as described in Hot-add and Hot-remove support for VMDirectPath I/O Devices.

- **You cannot set the Maximum Transmission Unit (MTU) on a VMware vSphere Distributed Switch to a value larger than 9174 on a Pensando DPU**

  If you have the vSphere Distributed Services Engine feature with a Pensando DPU enabled on your ESXi 8.0 system, you cannot set the Maximum Transmission Unit (MTU) on a vSphere Distributed Switch to a value larger than 9174.

  Workaround: None.

- **You see link flapping on NICs that use the ntg3 driver of version 4.1.3 and later**

  When two NICs that use the `ntg3` driver of versions 4.1.3 and later are connected directly, not to a physical switch port, link flapping might occur. The issue does not occur on `ntg3` drivers of versions earlier than 4.1.3 or the `tg3` driver. This issue is not related to the occasional Energy Efficient Ethernet (EEE) link flapping on such NICs. The fix for the EEE issue is to use a `ntg3` driver of version 4.1.7 or later, or disable EEE on physical switch ports.

  Workaround: Upgrade the `ntg3` driver to version 4.1.8 and set the new module parameter `noPhyStateSet` to `1`. The `noPhyStateSet` parameter defaults to `0` and is not required in most environments, except they face the issue.

- **You cannot use Mellanox ConnectX-5, ConnectX-6 cards Model 1 Level 2 and Model 2 for Enhanced Network Stack (ENS) mode in vSphere 8.0**

  Due to hardware limitations, Model 1 Level 2, and Model 2 for Enhanced Network Stack (ENS) mode in vSphere 8.0 is not supported in ConnectX-5 and ConnectX-6 adapter cards.

  Workaround: Use Mellanox ConnectX-6 Lx and ConnectX-6 Dx or later cards that support ENS Model 1 Level 2, and Model 2A.

- **Pensando DPUs do not support Link Layer Discovery Protocol (LLDP) on physical switch ports of ESXi hosts**

  When you enable LLDP on an ESXi host with a DPU, the host cannot receive LLDP packets.

  Workaround: None.

Storage Issues

- **VASA API version does not automatically refresh after upgrade to vCenter Server 8.0**

  vCenter Server 8.0 supports VASA API version 4.0. However, after you upgrade your vCenter Server system to version 8.0, the VASA API version might not automatically change to 4.0. You see the issue in 2 cases:

  a If a VASA provider that supports VASA API version 4.0 is registered with a previous version of VMware vCenter, the VASA API version remains unchanged after you upgrade to VMware vCenter 8.0. For example, if you upgrade a VMware vCenter system of version 7.x with a registered VASA provider that supports both VASA API versions 3.5 and 4.0, the VASA API version does not automatically change to 4.0, even though the VASA provider supports VASA API version 4.0. After the upgrade, when you navigate to **vCenter Server** > **Configure** > **Storage Providers** and expand the **General** tab of the registered VASA provider, you still see VASA API version 3.5.

  b If you register a VASA provider that supports VASA API version 3.5 with a VMware vCenter 8.0 system and upgrade the VASA API version to 4.0, even after the upgrade, you still see VASA API version 3.5.

Workaround: Unregister and re-register the VASA provider on the VMware vCenter 8.0 system.

- **Migration of a First Class Disk (FCD) might fail and the FCD remains in a tentative state**

  In certain scenarios, when you migrate a FCD to another datastore by invoking the `RelocateVStorageObject` API, the operation might intermittently fail and the FCD remains in a tentative state. As a result, you cannot complete any other operation on the FCD. For example, if you try another migration, in the backlog you see the error `com.vmware.vim.fcd.error.fcdAlreadyInTentativeState`.

  Workaround: Reconcile the source datastore of the FCD by following the steps described in VMware knowledge base article 2147750.

- **vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager**

  Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

  Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

- **You cannot create snapshots of virtual machines due to an error in the Content Based Read Cache (CBRC) that a digest operation has failed**

  A rare race condition when assigning a content ID during the update of the CBRC digest file might cause a discrepancy between the content ID in the data disk and the digest disk. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace. The snapshot creation task completes upon retry.

  Workaround: Retry the snapshot creation task.

vCenter Server and vSphere Client Issues

- **You see an error for Cloud Native Storage (CNS) block volumes created by using API in a mixed vCenter environment**

  If your environment has vCenter Server systems of version 8.0 and 7.x, creating Cloud Native Storage (CNS) block volume by using API is successful, but you might see an error in the vSphere Client, when you navigate to see the CNS volume details. You see an error such as `Failed to extract the requested data. Check vSphere Client logs for details. + TypeError: Cannot read properties of null (reading 'cluster')`. The issue occurs only if you review volumes managed by the 7.x vCenter Server by using the vSphere Client of an 8.0 vCenter Server.

Workaround: Log in to vSphere Client on a vCenter Server system of version 7.x to review the volume properties.

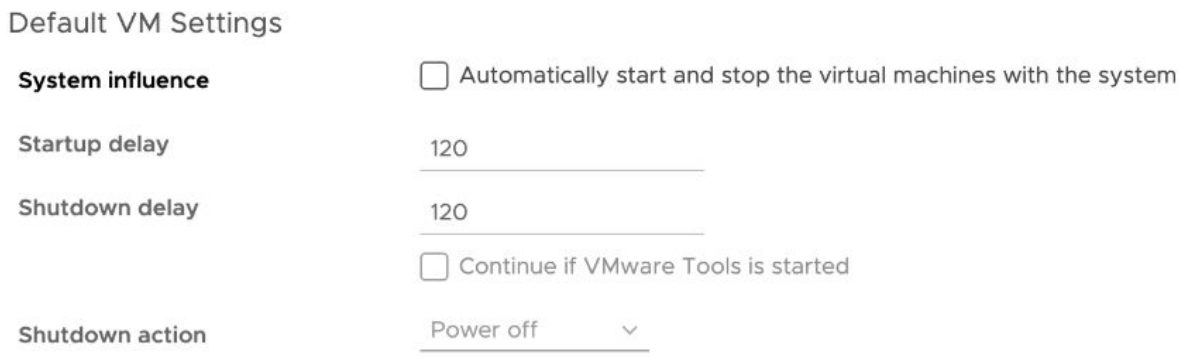
- **You see overlapped labels for parameters in the Edit VM Startup/Shutdown Configuration dialog box**

  In the vSphere Client, when you select an ESXi host and click **Configure** > **Virtual Machines** > **VM Startup/Shutdown** > **Edit**, you see overlapped labels for some parameters in the **Edit VM Startup/Shutdown Configuration** dialog box that opens. The overlapped labels are as follows:

  - System influence: labels the checkbox **Automatically start and stop the virtual machines with the system**.
  - Startup delay: numeric value that specifies the delay time that a host waits before powering on the next virtual machine in automatic startup configuration.
  - Shutdown delay: numeric value that defines the maximum time the ESXi host waits for a shutdown command to complete, and the option **Continue if VMware Tools is started**.
  - Shutdown action: such as Guest Shutdown, Power Off, Suspend, and None.

  Workaround: None. See the screenshot to figure out the sequence of labels:

  Figure 6-1.

- **VMware vCenter Lifecycle Manager might fail to load latest certificates and cannot complete a range of tasks**

  VMware vCenter Lifecycle Manager might fail to load the latest certificates when you opt for a non-disruptive certificate renewal in vCenter 8.0 Update 2. As a result, any functionality relying on vCenter Lifecycle Manager, which provides the underlying VMware vCenter Orchestration platform, such as the Update Planner, vSphere+ vCenter Lifecycle Management Service, and reduced downtime upgrade for vCenter, might fail.

  Workaround: Restart the vCenter Lifecycle Manager to get the latest certificates. For more information, see VMware knowledge base article 2109887.

- **ESXi hosts might become unresponsive, and you see a vpxa dump file due to a rare condition of insufficient file descriptors for the request queue on vpxa**

In rare cases, when requests to the vpxa service take long, for example waiting for access to a slow datastore, the request queue on vpxa might exceed the limit of file descriptors. As a result, ESXi hosts might briefly become unresponsive, and you see a `vpxa-zdump.00*` file in the `/var/core` directory. The vpxa logs contain the line `Too many open files`.

Workaround: None. The vpxa service automatically restarts and corrects the issue.

- **You do not see the option to push root certificates to vCenter hosts**

  In the **Add Trusted Root Certificate** screen under the **Certificate Management** tab in the vSphere Client, you do not see the option **Start Root certificate push to vCenter Hosts**.

  Workaround: This change in the **Add Trusted Root Certificate** screen is related to the non-disruptive certificate management capability introduced with vCenter 8.0 Update 2 and is expected. For more information, see Non-disruptive Certificate Management.

- **If you use custom update repository with untrusted certificates, vCenter Server upgrade or update by using vCenter Lifecycle Manager workflows to vSphere 8.0 might fail**

  If you use a custom update repository with self-signed certificates that the VMware Certificate Authority (VMCA) does not trust, vCenter Lifecycle Manager fails to download files from such a repository. As a result, vCenter Server upgrade or update operations by using vCenter Lifecycle Manager workflows fail with the error `Failed to load the repository manifest data for the configured upgrade`.

  Workaround: Use CLI, the GUI installer, or the Virtual Appliance Management Interface (VAMI) to perform the upgrade. For more information, see VMware knowledge base article 89493.

- **A scheduled task fails and doesn't schedule further runs**

  With vSphere 8.0 Update 2, if a vCenter user is unauthorized or unauthenticated, all scheduled tasks they own fail and cannot be scheduled until the user privileges are restored or a different vSphere user takes over the scheduled tasks. In the vSphere Client, you see messages for failed tasks and reasons for the failure.

  Workaround: Any vSphere user with sufficient privileges to edit scheduled tasks, including the current task owner with restored privileges, can click **Edit** and submit the scheduled task, without actually changing the scheduled task. For more information, see Scheduling vSphere Tasks.

Virtual Machine Management Issues

- **When you add an existing virtual hard disk to a new virtual machine, you might see an error that the VM configuration is rejected**

  When you add an existing virtual hard disk to a new virtual machine by using the VMware Host Client, the operation might fail with an error such as `The VM configuration was rejected. Please see browser Console`. The issue occurs because the VMware Host Client might fail to get some properties, such as the hard disk controller.

Workaround: After you select a hard disk and go to the **Ready to complete** page, do not click **Finish**. Instead, return one step back, wait for the page to load, and then click **Next** > **Finish**.

- **In a mixed vCenter environment, when you clone a VM with First Class Disk (FCD) attached and delete it, the attached FCD in the cloned VM is also deleted**

  In a mixed vCenter environment, where vCenter is on version 8.0 Update 2 or later and ESXi is on version 7.0 Update 3 or earlier, when you clone a VM with FCD, the parameter `KeepAfterDeleteVM` is set to `FALSE` by default. As a result, if the cloned VM is deleted, the attached cloned FCD is also deleted.

  Workaround: In a mixed vCenter environment, where vCenter is of version 8.0 Update 2 or later and ESXi is on version 7.0 Update 3 or earlier, set the `KeepAfterDeleteVM` parameter to `TRUE` by using the FCD API : `setVStorageObjectControlFlags`. You can invoke the FCD API at `https://<VC_IP>/mob/?moid=VStorageObjectManager&method=setVStorageObjectControlFlags` and pass the control flag : `KeepAfterDeleteVM`.

vSphere Lifecycle Manager Issues

- **You do not see a warning or error when entering non-numeric values for a desired cluster configuration setting in the vSphere Client that requires numbers**

  When you edit the host settings of the draft configuration for a cluster that uses vSphere Configuration Profiles, you can enter non-numeric values in a field that expects only numbers and you see no error or warning. For example, if you set non-numeric characters in the setting for syslog rotations, `esx/syslog/global_settings/rotations`, which expects a number, the **Edit** dialog box closes without an error and seems to save the value, but the setting actually keeps the previous valid value.

  Workaround: Use numeric values in fields that expect numbers. Use numbers in text inputs that expect numbers.

- **You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task**

  In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

  Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

- **Manually applied security advanced options on a vCenter system might not persist across vSphere Lifecycle Manager operations**

  Some of all manually applied security advanced options on a vCenter system might not persist across vSphere Lifecycle Manager operations, such as upgrade, update, backup, or restore.

Workaround: Re-apply the manual settings after the vSphere Lifecycle Manager task completes.

- **If a parallel remediation task fails, you do not see the correct number of ESXi hosts that passed or skipped the operation**

  With vSphere 8.0, you can enable vSphere Lifecycle Manager to remediate all hosts that are in maintenance mode in parallel instead of in sequence. However, if a parallel remediation task fails, in the vSphere Client you might not see the correct number of hosts that passed, failed, or skipped the operation, or even not see such counts at all. The issue does not affect the vSphere Lifecycle Manager functionality, but only the reporting in the vSphere Client.

  Workaround: None.

- **You see an authentication error on the vSphere Lifecycle Manager home view in one of several linked vCenter instances**

  After an update of a linked vCenter system, access to the vSphere Lifecycle Manager home page in the vSphere Client from one of the linked vCenter instances might fail. When you select **Menu > Lifecycle Manager**, you see the error `Authentication failed, Lifecycle Manager server could not be contacted`. The issue also affects vSphere Lifecycle Manager baseline pages and workflows. Workflows with vSphere Lifecycle Manager images are not affected.

  Workaround: Log in to the vSphere Client from another vCenter instance in the linked environment or restart the **vsphere-ui** service to resolve the issue.

- **You see error messages when try to stage vSphere Lifecycle Manager Images on ESXi hosts of version earlier than 8.0**

  ESXi 8.0 introduces the option to explicitly stage desired state images, which is the process of downloading depot components from the vSphere Lifecycle Manager depot to the ESXi hosts without applying the software and firmware updates immediately. However, staging of images is only supported on an ESXi 8.0 or later hosts. Attempting to stage a vSphere Lifecycle Manager image on ESXi hosts of version earlier than 8.0 results in messages that the staging of such hosts fails, and the hosts are skipped. This is expected behavior and does not indicate any failed functionality as all ESXi 8.0 or later hosts are staged with the specified desired image.

  Workaround: None. After you confirm that the affected ESXi hosts are of version earlier than 8.0, ignore the errors.

- **A remediation task by using vSphere Lifecycle Manager might intermittently fail on ESXi hosts with DPUs**

  When you start a vSphere Lifecycle Manager remediation on an ESXi hosts with DPUs, the host upgrades and reboots as expected, but after the reboot, before completing the remediation task, you might see an error such as:

`A general system error occurred: After host … remediation completed, compliance check reported host as 'non-compliant'. The image on the host does not match the image set for the cluster. Retry the cluster remediation operation.`

This is a rare issue, caused by an intermittent timeout of the post-remediation scan on the DPU.

Workaround: Reboot the ESXi host and re-run the vSphere Lifecycle Manager compliance check operation, which includes the post-remediation scan.

VMware Host Client Issues

- **VMware Host Client might display incorrect descriptions for severity event states**

  When you look in the VMware Host Client to see the descriptions of the severity event states of an ESXi host, they might differ from the descriptions you see by using Intelligent Platform Management Interface (IPMI) or Lenovo XClarity Controller (XCC). For example, in the VMware Host Client, the description of the severity event state for the PSU Sensors might be `Transition to Non-critical from OK`, while in the XCC and IPMI, the description is `Transition to OK`.

  Workaround: Verify the descriptions for severity event states by using the ESXCLI command `esxcli hardware ipmi sdr list` and Lenovo XCC.

Security Features Issues

- **If you use an RSA key size smaller than 2048 bits, RSA signature generation fails**

  Starting from vSphere 8.0, ESXi uses the OpenSSL 3.0 FIPS provider. As part of the FIPS 186-4 requirement, the RSA key size must be at least 2048 bits for any signature generation, and signature generation with SHA1 is not supported.

  Workaround: Use RSA key size larger than 2048.

- **You cannot encrypt virtual machines when connected to a vCenter version earlier than 8.0 Update 1**

  When you use the vSphere Client to connect to a vCenter system of version 7.x or earlier than 8.0 Update 1, and try to encrypt a VM either in the **New Virtual Machine** wizard or in the **Edit Settings** dialog of an existing VM, you see errors such as `Operation failed! RuntimeFault.Summary and A general runtime error occurred. Key /default KMS cluster not found`. The task completes successfully when you use the vSphere Client to log in to a vCenter system of version 8.0 Update 1 or later.

  Workaround: Use the vSphere Client from the vCenter instance of version earlier than 8.0 Update 1 to encrypt the VM. Alternatively, you can enable VM encryption on another vCenter instance of version 8.0 Update 1 and later, and migrate the already encrypted VM to the vCenter instance of earlier version.