VMware vSphere 8.0 Release Notes

VMware vSphere 8.0
ESXi 8.0
vCenter Server 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 vSphere 8.0 | 11 OCT 2022
ESXi 8.0 | 11 OCT 2022 | Build 20513097
vCenter Server 8.0 | 11 OCT 2022 | Build 20519528
Check for additions and updates to these release notes.

What's New

2

- This release of VMware vSphere 8.0 includes VMware ESXi 8.0 and VMware vCenter Server 8.0. Read about the new and enhanced features in this release in the vSphere 8 Technical Overview Blog.

  The vSphere 8.0 release notes do not include the following release notes:

  - VMware vSphere With Tanzu
  - Tanzu Kubernetes releases
  - VMware vSAN
  - VMware Host Client

General Availability

3

- vSphere 8.0 is designated General Availability (GA). Custom ISO images that use ESXi 8.0 GA as a base image and include OEM firmware and drivers are available.

  For more information, read the vSphere 8 General Availability blog.

  IMPORTANT: Do not upgrade to this release if you use the Tanzu Kubernetes Grid service (TKG guest clusters) on vSphere along with the NSX Advanced Load Balancer (formerly known as Avi Networks) and have multiple Service Engine Groups configured. Upgrading to VMware vSphere with Tanzu 8.0 for such environments might result in failure to create new Tanzu Kubernetes guest clusters or cause upgrades of existing Supervisor Clusters to fail.

Internationalization

4

- **VMware vSphere 8.0 is available in the following languages:**
  - English
  - Italian
  - French
  - German
  - Spanish
  - Japanese
  - Korean
  - Simplified Chinese
  - Traditional Chinese

  Components of vSphere 8.0, including vCenter Server, ESXi, the vSphere Client, and the VMware Host Client, do not accept non-ASCII input.

Compatibility

5

- **Virtual Machine Compatibility for ESXi**

  Virtual machines that are compatible with ESX 3.x and later (hardware version 4) are supported with ESXi 8.0. Virtual machines that are compatible with ESX 2.x and later (hardware version 3) are not supported. To use such virtual machines on ESXi 8.0, upgrade the virtual machine compatibility. See the ESXi Upgrade documentation.

- **Guest Operating System Compatibility for ESXi**

  To determine which guest operating systems are compatible with vSphere 8.0, use the ESXi 8.0 information in the VMware Compatibility Guide.

  The following guest operating system releases are deprecated or terminated in this release. Future vSphere releases will not support these guest operating systems:

  - Windows Vista, Windows 2003 / R2, Windows XP: Deprecated
  - Oracle Linux 5.x: Deprecated
  - Oracle Linux 4.9: Terminated
  - CentOS 5.x: Deprecated
  - Asianux 3.0: Deprecated
  - SUSE Linux Enterprise Server 9 SP4: Terminated
  - SUSE Linux Enterprise Server 10 SP4: Deprecated
  - SUSE Linux Enterprise Desktop 12: Deprecated
  - Ubuntu releases 12.04, 18.10, 19.04 and 19.10: Terminated
  - Debian 7.x and 8.x: Deprecated
  - Debian 6.0: Terminated
  - Photon OS 1.0: Terminated
  - Flatcar Container Linux non-LTS releases: Terminated
  - All OS X and macOS releases: Terminated
  - FreeBSD 9.x and 10.x: Deprecated

- FreeBSD 7.x and 8.x: Terminated
- Solaris 10.x: Deprecated
- All eComStation releases: Terminated
- All SCO releases: Terminated
- All CoreOS releases: Terminated

- **Device Compatibility for ESXi**

  To determine which devices are compatible with ESXi 8.0, use the ESXi 8.0 information in the VMware Compatibility Guide.

- **Hardware Compatibility for ESXi**

  To view a list of processors, storage devices, SAN arrays, and I/O devices that are compatible with vSphere 8.0, use the ESXi 8.0 information in the VMware Compatibility Guide.

- **ESXi and vCenter Server Version Compatibility**

  The VMware Product Interoperability Matrix provides details about the compatibility of current and earlier versions of VMware vSphere components, including ESXi, VMware vCenter Server, and optional VMware products. Check the VMware Product Interoperability Matrix also for information about supported management and backup agents before you install ESXi or vCenter Server.

  The vSphere Lifecycle Manager and vSphere Client are packaged with vCenter Server.

Before You Begin

6

- vSphere 8.0 requires one CPU license for up to 32 physical cores. If a CPU has more than 32 cores, additional CPU licenses are required as announced in Update to VMware's per-CPU Pricing Model. Prior to upgrading ESXi hosts, you can determine the number of licenses required using the license counting tool described in Counting CPU licenses needed under new VMware licensing policy.

Installation and Upgrades for This Release 7

- **VMware Tools Bundling Changes in ESXi 8.0**
  - The following VMware Tools ISO images are bundled with ESXi 8.0:
    - **windows.iso**: VMware Tools 12.0.6 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
    - **linux.iso**: VMware Tools 10.3.24 ISO image for Linux OS with `glibc` 2.11 or later.

    The following VMware Tools ISO images are available for download:
    - VMware Tools 11.0.6:
      - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
    - VMware Tools 10.0.12:
      - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
      - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with `glibc` version earlier than 2.5.
    - **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
    - **darwin.iso**: Supports Mac OS X versions 10.11 and later.

    Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:
    - VMware Tools 12.0.6 Release Notes
    - Earlier versions of VMware Tools
    - What Every vSphere Admin Must Know About VMware Tools
    - VMware Tools for hosts provisioned with Auto Deploy
    - Updating VMware Tools
- **Installation Notes**

Read the ESXi Installation and Setup and the vCenter Server Installation and Setup documentation for guidance about installing and configuring ESXi and vCenter Server.

Although the installations are straightforward, several subsequent configuration steps are essential. Read the following documentation:

"License Management" in the vCenter Server and Host Management documentation

"Networking" in the vSphere Networking documentation

"Security" in the vSphere Security documentation for information on firewall ports

VMware's Configuration Maximums tool helps you plan your vSphere deployments. Use this tool to view the limits for virtual machines, ESXi, vCenter Server, vSAN, networking, and others. You can also compare limits for two or more product releases. The VMware Configuration Maximums tool is best viewed on larger format devices such as desktops and laptops.

- **Deprecation of USB or SD card devices for full ESXi installation:** Starting with ESXi 8.0, legacy SD and USB devices are supported with limitations and certification of new platforms with SD cards is not supported. SD and USB devices are supported for boot bank partitions. You can find a list of validated devices on partnerweb.vmware.com. The use of SD and USB devices for storing ESX-OSData partitions is being deprecated and the best practice is to provide a separate persistent local device with a minimum of 32 GB to store the ESX-OSData volume. For more details, see VMware knowledge base article 85685.
- **ESXi boot memory requirements increased:** The minimum memory requirements for ESXi to boot have increased from 4GB to 8GB. The minimum amount of memory needed to run VMs remains unchanged at 8GB.
- **The 'reboot -f' option is not supported for ESXi installation with a DPU:** Although ESXi supports the `-f force` reboot option, if you use `reboot -f` on an ESXi configuration with a DPU, the forceful reboot might cause an invalid state.
- You cannot install ESXi on DPUs by using Auto Deploy. You can use the interactive and scripted methods for fresh installations of ESXi on DPU.

- **Upgrades and Installations Disallowed for Unsupported CPUs**
  - For ESXi hosts using Broadcom `bnxtnet` NIC drivers, make sure the NIC firmware is a compatible version such as 222.1.68.0 or higher, before you install or upgrade to ESXi 8.0. If you do not use a compatible firmware version, as specified in the VMware Compatibility Guide, or as recommend by the OEM, you might see issues such as a drop in performance, firmware failure or ESXi host failure.
  - vSphere 8.0 no longer supports CPUs which have been marked as End of Support or End of Life from hardware vendors. For more details, see VMware knowledge base article 82794.

- **Deprecation of legacy BIOS:** In vSphere 8.0, booting ESXi hosts with the Unified Extensible Firmware Interface (UEFI) is strongly recommended. Some ESXi 8.0 hosts might not successfully boot in legacy BIOS mode. If this change affects your vSphere system, see VMware knowledge base articles 84233 and 89682 for details and action plans.

- **Upgrade notes**
  - Best practice for vSphere system upgrades is that the vCenter version is always greater than or equal to the ESXi version to ensure that you can use all new capabilities introduced with the latest vSphere release. For more information about vSphere build numbers, see Build numbers and versions of VMware vCenter Server and Build numbers and versions of VMware ESXi/ESX. For vSphere back-in-time release upgrade restrictions, see VMware knowledge base article 67077.
  - Before upgrading vCenters in Enhanced Link Mode (ELM), best practice is to create powered-off concurrent snapshots for all vCenter Servers and Platform Services Controllers within the Single Sign-On domain to prevent replication sync issues. If a rollback to snapshot is necessary, all PSC and vCenter Servers can be reverted to the previous state.
  - vSphere 8.0 is not compatible with VMware NSX for vSphere (NSX-V). Upgrade paths to vSphere 8.0 from systems featuring NSX for vSphere are not supported. For more information, see the NSX Migration Guide.
  - Direct upgrade from ESXi 6.5 to 8.0 is not supported, because VMKAPI version 2.4, introduced in ESXi 6.5, is removed from ESXi 8.0. If you have ESXi 6.5 VIBs that depend on VMKAPI version 2.4 in a 6.7.x or 7.x environment, such VIBs prevent upgrade from 6.7.x or 7.x to 8.0. You must use only VIBs of version 6.7.x or later in the image that you use for upgrade to ESXi 8.0. To provide newer versions of the VIBs, you can recertify with the corresponding development kit for versions of VMKAPI later than 2.4. For more information, see VMware knowledge base article 88646.
  - If you proceed to upgrade to ESXi 8.0 from a host with a device supported by the `nmlx4_en` driver, or a device removed in the `lpfc` driver, the following non-recoverable consequences can occur: lose access to storage or datastores, lose network access, or lose previous configuration on the host. Before upgrading to ESXi 8.0, you should replace devices previously supported by the `nmlx4_en` driver or devices that have been removed in the 8.0 `lpfc` driver. For the full list of devices no longer supported in ESXi 8.0, see VMware knowledge base article 88172.
  - ESXi 8.0 installation and upgrade workflows block VIBs that do not have SHA256 checksum in their metadata, such as VIBs of ESXi version earlier than 6.7. You must replace such VIBs with later versions: 6.7.x, 7.x and 8.0.

- ESXi upgrade on DPUs is not supported by the interactive or scripted method. Instead, you can use vSphere Lifecycle Manager or ESXCLI. For example, an `esxcli software *` command run on an ESXi host automatically triggers the same operation on the DPU if such is present on the host.

Open Source Components for vSphere 8.0

8

After you log in to your Customer Connect account, the copyright statements and licenses applicable to the open source software components distributed in vSphere 8.0 are available at https://customerconnect.vmware.com/en/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/8_0#open_source. On the **Open Source** tab, you can also download the source files for any GPL, LGPL, or other similar licenses that require the source code or modifications to source code to be made available for the most recent available release of vSphere.

Product Support Notices

9

-
  - **Data Processing Unit (DPU) Support:** vSphere 8.0 adds support for NVIDIA and AMD Pensando SmartNIC devices, also called DPUs, in ESXi. For more information, see Introducing VMware vSphere® Distributed Services Engine™ and Networking Acceleration by Using DPUs.
  - **TPM provision policy:** Starting with ESX 8.0, you can use the TPM provision policy where virtual TPM devices can be automatically replaced during clone or deployment operations. For more information, see Windows 11 Support on vSphere.
  - **Deprecation of N-Port ID Virtualization (NPIV):** NPIV, which is an ANSI T11 standard that defines how to register a single Fibre Channel HBA port with the fabric by using several worldwide port names (WWPNs), will be deprecated in a future release of vSphere due to many existing alternatives.
  - **Deprecation of Integrated Windows Authentication (IWA):** Due to performance issues with IWA-based authentication, vSphere 8.0 deprecates the use of IWA. You can use AD over LDAP or ADFS.
  - **Deprecation of Common Information Model (CIM) and Service Location Protocol (SLP):** Support for CIM and SLP is deprecated in ESXi 8.0 due to security issues and will be removed in a future release. As an alternative, consider using the Daemon Software Development Kit (DSDK) for solutions that rely on CIM, such as the CIM Provider Development Kit (CIMPDK) and the vSphere APIs for I/O Filtering (VAIO) Development Kit. No CIMPDK is released for vSphere 8.0, but CIM Providers for ESXi 7.x. continue to work on ESXi 8.0 to support a smooth upgrade process.
  - **Smart Card mutual authentication moves to port 3128**: vCenter Server 8.0 moves the Smart Card mutual authentication to port 3128 and requires a restart of the Security Token Service (STS) during configuration. For more information, see Configure the Reverse Proxy to Request Client Certificates.
  - VMware inbox `qedentv` NIC driver from Marvell does not support NVMe/TCP in Enhanced Networking Stack (ENS) mode in ESXi 8.0.

- **Deprecation of vSphere Lifecycle Manager baselines:** Managing clusters with vSphere Lifecycle Manager baselines and baseline groups (legacy vSphere Update Manager workflows) is supported in vSphere 8.0, but support will drop in a future vSphere release. Instead of baselines and baseline groups, you can use vSphere Lifecycle Manager images to perform tasks on a cluster level such as install a desired ESXi version on all hosts in a cluster, install and update third-party software, update, and upgrade ESXi or firmware, generate recommendations, and use a recommended image for your cluster. For more details, see the blog Introducing vSphere Lifecycle Management (vLCM).
- **Predefined vSphere Lifecycle Manager baselines restriction to VMware content only**: As of vSphere 8.0, vSphere Lifecycle Manager predefined baselines are restricted only to VMware-provided content. Third-party content such as async drivers and tools no longer can be part of predefined baselines. If you need to add third-party content to update baselines, you must manually create custom baselines.
- **Deprecation of Patch Manager APIs:** With vSphere 8.0, Patch Manager APIs are deprecated. Patch Manager APIs are supported in vSphere 8.0, but support will discontinue in a future release of vSphere. Instead of Patch Manager APIs, you can use the latest vSphere APIs, documented in the vSphere API automation reference guide.
- **Deprecation of local plug-ins:** Moving vSphere plug-ins to a remote plug-in architecture, vSphere 8.0 deprecates support for local plug-ins. VMware plans to discontinue support for local plug-ins in a future vSphere release. For more information, see the blog Deprecating the Local Plugins :- The Next Step in vSphere Client Extensibility Evolution and VMware knowledge base article 87880.
- **Removal of support for 32-bit userworlds:** ESXi 8.0 does not support 32-bit user worlds and you need to recompile any solution using the 32-bit subsystem.
- **Removal of VMKAPI v2.4:** vSphere 8.0 does not support VMKAPI v2.4 and you must use newer versions of the API and recertify with the latest development kit.
- **Removal of nmlx4_en driver:** ESXi 8.0 removes the `nmlx4_en` driver and all devices for this driver are not supported.
- **Removal of Trusted Platform Module (TPM) 1.2:** VMware discontinues 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.
- **Removal of insecure ciphers:** X.509 certificates that specify a SHA-1 signature algorithm, or other weak signature algorithms, are no longer supported in vSphere 8.0. Prechecks prevent upgrade to vCenter Server 8.0 and ESXi 8.0 if certificates with a weak signature algorithm are in use. For remediation steps, see VMware knowledge base article 89424.
- **Removal of Software FCoE Adapters:** In vSphere 8.0, the option to configure software FCoE adapters that use the native FCoE stack in ESXi is removed and not supported. The change does not impact hardware FCoE adapters and drivers.

- **Discontinuation of support for I/O devices used by nmlx4_en and lpfc drivers:** VMware intends to discontinue support for I/O devices that reach EOL, such as devices previously supported by the `lpfc` driver and all devices for the `nmlx4_en` driver. For more information, see VMware knowledge base article 88172.
- **You cannot register a read-only VMDK as FCD:** In vSphere 8.0, any Virtual Storage Lifecycle Management API invoked on read only vmdk registered as FCD is not supported.
- **Discontinuation of support for Guest OS:** vSphere 8.0 drops support for the following guest operating systems:
  - eComStation
  - SCO Openserver
  - SCO Unixware
  - Oracle Linux 4.x
  - SLES9 SP4
  - Ubuntu 12.04 LTS
  - Debian 6.0
  - FreeBSD 7.x
  - FreeBSD 8.x
- **Prevent execution of untrusted binaries:** Starting with ESXi 8.0, a new security option has been turned on by default to limit execution of untrusted binaries to better protect against ransomware attacks. The `execInstalledOnly` option is now a run time parameter which limits execution of binaries such as applications and vmkernel modules to improve security and guard against breaches and compromises. When `execInstalledOnly` is enabled, only binaries that are installed locally by using a VIB will be allowed to run.
- **OpenSSL 3.0 support:** ESXi 8.0 supports OpenSSL 3.0 and drops support for TLS 1.0 and TLS 1.1. vCenter does not support OpenSSL 3.0. In vCenter, TLS 1.2 is enabled by default and TLS 1.0, and TLS 1.1 are disabled by default, but you can temporarily enable them.
- **Hardware timestamp-based Precision Time Protocol (PTP) certification for NICs:** vSphere 8.0 adds certification for NICs that support hardware timestamp-based PTP as part of the I/O Vendor Partner (IOVP) certification program.
- **NVMe over Fabrics (NVMe-oF) support for vSphere Virtual Volumes:** vSphere 8.0 adds NVMe-oF support for vSphere Virtual Volumes as part of the IOVP NVMe-FC certification program.
- **NVMeoF-RDMA scale enhancements:** With NVMeoF, you can scale NVMe namespaces and paths to 256 and 4,000 respectively in vSphere 8.0.
- **Advanced NVMe-oF Discovery Service Support:** vSphere 8.0 adds dynamic discovery of devices for compliant NVMe Discovery Services and Storage Arrays.

- **Syslog enhancements:** vSphere 8.0 unifies the format of logs by the ESXi syslog daemon across all of vSphere and VCF products and if your system consumes syslog log files directly from ESXi, you need to update your solutions. For more information, see Configuring System Logging. You can optionally configure transmissions of syslog messages from ESXi in compliance with RFC 5424 or frame messages. For more information, see Protocols, Formats and Framing of ESXi Syslog Messages. You can set all syslog controlling parameters by using either the vSphere Client or the VMware Host Client and do not need to use SSH or ESXCLI.
- **Phasing out LSI SAS controllers:** vSphere 8.0 can automatically and safely replace the LSI SAS controller for VMs on Windows 10 and later or Windows Server 2016 and later with the native VMware PVSCI controller, because the LSI SAS driver for Windows has reached end of life. For VMs on versions earlier than Windows 10 and Windows Server 2016, you can manually replace the LSI SAS controller with PVSCI, SATA, or a NVMe controller.
- **Compliance of the default RSA key length with U.S. Department of Defense Impact Level 6 (IL-6):** To conform with IL6 standards, the default RSA key length generated for vCenter Server certificates increases to 3072 bits in vSphere 8.0 from 2048 bits.
- **Administer user access to ESXi Shell:** Starting with vSphere 8.0, users with the Administrator role can remove or grant ESXi Shell access to user accounts. For more information, see How Do You Configure a Security vSphere Host Profile.
- **Discontinuation of support for Apple Mac platforms:** ESXi 8.0 does not support Apple MacPro and Apple MacMini platforms, and macOS as a guest operating system. For more information, see VMware knowledge base article 88698.
- **Virtual hardware version 20:** ESXi 8.0 introduces virtual hardware version 20 to enable support for virtual machines with higher resource maximums, and:
  - Virtual NUMA Topology
  - Enhanced Direct Path I/O
  - Virtual Hyperthreading
  - vMotion App Notification
  - VM DataSets
  - OpenGL 4.3
  - UEFI 2.7A
- **Increased scalability with vSphere Lifecycle Manager:** With vSphere 8.0, scalability for operations with vSphere Lifecycle Manager images increases to 1,000 ESXi hosts from 280.
- **Support for UEFI 2.7A:** vSphere 8.0 complies with UEFI specification version 2.7A to support some Microsoft Windows 11 features.

- **vSphere Configuration Profiles**: vSphere 8.0 launches vSphere Configuration Profiles in tech preview. This capability allows you to manage ESXi cluster configurations by specifying a desired host configuration at the cluster level, automates the scanning of ESXi hosts for compliance to the specified Desired Configuration and remediates any host that is not compliant. The tech preview launch is applicable only to customers that use standard switches and does not support VMware vSphere Distributed Switch (VDS) and requires that you use vSphere Lifecycle Manager images to manage your cluster lifecycle.
- **Removal of RDMA over Converged Ethernet (RoCE) v1**: Starting with vSphere 8.0, VMware does not support the network protocol RoCE v1. You can use RoCEv2. Make sure you migrate your paravirtualized remote direct memory access (PVRDMA) network adapters for virtual machines and guest operating systems to an adapter that supports RoCEv2.

Known Issues

10

Read the following topics next:

Installation, Upgrade, and Migration Issues

- **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.

- **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.

- **If a vCenter Server Security Token Service (STS) refresh happens during upgrade to ESXi 8.0, the upgrade might fail**

  In vSphere 8.0, vCenter Single Sign-On automatically renews a VMCA-generated STS signing certificate. The auto-renewal occurs before the STS signing certificate expires and before triggering the 90-day expiration alarm. However, in long-running upgrade or remediation tasks by using a vSphere Lifecycle Manager image on multiple ESXi hosts in a cluster, vSphere Lifecycle Manager might create a cache of STS certificates internally. In very rare cases, if an STS certificates refresh task starts in parallel with the long-running upgrade or remediation task, the upgrade task might fail as the STS certificates in the internal cache might be different from the refreshed certificates. After the upgrade task fails, some ESXi hosts might remain in maintenance mode.

  Workaround: Manually exit any ESXi hosts in maintenance mode and retry the upgrade or remediation. Refreshing or importing and replacing the STS signing certificates happens automatically and does not require a vCenter Server restart, to avoid downtime.

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

  If the peer physical switch of a VMNIC does not support the auto negotiate option, or the option is deactivated, 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.

- **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.

- **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.

Miscellaneous Issues

- **Reset or restore of the ESXi system configuration in a vSphere system with DPUs might cause invalid state of the DPUs**

  If you reset or restore the ESXi system configuration in a vSphere system with DPUs, for example, by selecting **Reset System Configuration** in the direct console, the operation might cause invalid state of the DPUs. In the DCUI, you might see errors such as `Failed to reset system configuration. Note that this operation cannot be performed when a managed DPU is present`. A backend call to the `-f` force reboot option is not supported for ESXi installations with a DPU. Although ESXi 8.0 supports the `-f` force reboot option, if you use `reboot -f` on an ESXi configuration with a DPU, the forceful reboot might cause an invalid state.

  Workaround: Reinstall ESXi. Avoid resetting the ESXi system configuration in a vSphere system with DPUs.

- **In the vSphere API Explorer, VMware Datacenter CLI (DCLI) and PowerCLI, you see an API option "contentinternal" that is not functional**

  You see an API option **contentinternal** in the metadata of either the vSphere API Explorer, DCLI and PowerCLI. For example, when you open `https://<your vCenter IP>/ui/app/devcenter/api-explorer`, you see the option in the **select API** drop-down menu. This option is not functional.

  Workaround: Ignore the **contentinternal** API option and do not use it.

- **If you configure a VM at HW version earlier than 20 with a Vendor Device Group, such VMs might not work as expected**

  Vendor Device Groups, which enable binding of high-speed networking devices and the GPU, are supported only on VMs with HW version 20 and later, but you are not prevented to configure a VM at HW version earlier than 20 with a Vendor Device Group. Such VMs might not work as expected: for example, fail to power-on.

Workaround: Ensure that VM HW version is of version 20 before you configure a Vendor Device Group in that VM.

- **If you deploy a virtual machine from an OVF file or from the Content Library, the number of cores per socket for the VM is set to 1**

  If you deploy a virtual machine from an OVF file or from the Content Library, instead of ESXi automatically selecting the number of cores per socket, the number is pre-set to 1.

  Workaround: You can manually set the number of cores per socket by using the vSphere Client.

- **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: None.

- **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.

- **Some ionic_en driver uplinks might work with just a single receive queue and you see slower performance in native mode**

Pensando Distributed Services Platform (DSC) adapters have 2 high speed ethernet controllers (for example `vmnic6` and `vmnic7`) and one management controller (for example `vmnic8`):

```
:~] esxcfg-nics -l

vmnic6 0000:39:00.0 ionic_en_unstable Up 25000Mbps Full 00:ae:cd:09:c9:48 1500
Pensando Systems DSC-25 10/25G 2-port 4G RAM 8G eMMC G1 Services Card, Ethernet
Controller

vmnic7 0000:3a:00.0 ionic_en_unstable Up 25000Mbps Full 00:ae:cd:09:c9:49 1500
Pensando Systems DSC-25 10/25G 2-port 4G RAM 8G eMMC G1 Services Card, Ethernet
Controller

:~] esxcfg-nics -lS

vmnic8 0000:3b:00.0 ionic_en_unstable Up 1000Mbps Full 00:ae:cd:09:c9:4a 1500
Pensando Systems DSC-25 10/25G 2-port 4G RAM 8G eMMC G1 Services Card, Management
Controller
```

The high-speed ethernet controllers `vmnic6` and `vmnic7` register first and operate with RSS set to 16 receive queues.

```
:~] localcli --plugin-dir /usr/lib/vmware/esxcli/int networkinternal nic privstats
get -n vmnic6…Num of RSS-Q=16, ntxq_descs=2048, nrxq_descs=1024, log_level=3,
vlan_tx_insert=1, vlan_rx_strip=1, geneve_offload=1 }
```

However, in rare cases, if the management controller `vmnic8` registers first with the vSphere Distributed Switch, the high-speed ethernet controllers `vmnic6` or `vmnic7` uplink might end up operating with RSS set to 1 receive queue.`:~] localcli --plugin-dir /usr/lib/vmware/esxcli/int networkinternal nic privstats get -n vmnic6…Num of RSS-Q=1, ntxq_descs=2048, nrxq_descs=1024, log_level=3, vlan_tx_insert=1, vlan_rx_strip=1, geneve_offload=1 }`

As a result, you might see slower performance in native mode.

Workaround: Reload the `ionic_en driver` on ESXi by using the following commands:`:~] esxcfg-module -u ionic_en:~] esxcfg-module ionic_en:~] localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal bind`.

- **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.

- **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.

- **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.

- **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.

- **If a PCI passthrough is active on a DPU during the shutdown or restart of an ESXi host, the host fails with a purple diagnostic screen**

  If an active virtual machine has a PCI passthrough (SR-IOV or UPT) to a DPU at the time of shutdown or reboot of an ESXi host, the host fails with a purple diagnostic screen. The issue is specific for systems with DPUs and only in case of VMs that use PCI passthrough to the DPU.

Workaround: Before shutdown or reboot of an ESXi host, make sure the host is in maintenance mode, or that no VMs that use PCI passthrough to a DPU are running. If you use auto start options for a virtual machine, the Autostart manager stops such VMs before shutdown or reboot of a host.

Networking Issues

- **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.

- **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.

- **If you do not reboot an ESXi host after you enable or disable SR-IOV with the icen driver, when you configure a transport node in ENS Interrupt mode on that host, some virtual machines might not get DHCP addresses**

  If you enable or disable SR-IOV with the `icen` driver on an ESXi host and configure a transport node in ENS Interrupt mode, some Rx (receive) queues might not work if you do not reboot the host. As a result, some virtual machines might not get DHCP addresses.

  Workaround: Either add a transport node profile directly, without enabling SR-IOV, or reboot the ESXi host after you enable or disable SR-IOV.

- **VMware NSX installation or upgrade in a vSphere environment with DPUs might fail with a connectivity error**

  An intermittent timing issue on the ESXi host side might cause NSX installation or upgrade in a vSphere environment with DPUs to fail. In the `nsxapi.log` file you see logs such as `Failed to get SFHC response. MessageType MT_SOFTWARE_STATUS`.

  Workaround: Wait for 10 min and retry the NSX install or upgrade.

- **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 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.

Storage Issues

- **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.

- **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.

- **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.

vCenter Server and vSphere Client Issues

- **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 90259.

- **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 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.

- **In the vSphere Client, you do not see banner notifications for historical data imports**

  Due to a backend issue, you do not see banner notifications for background migration of historical data in the vSphere Client.

  Workaround: Use the vCenter Server Management Interface as an alternative to the vSphere Client. For more information, see Monitor and Manage Historical Data Migration.

- **If you load the vSphere virtual infrastructure to more than 90%, ESXi hosts might intermittently disconnect from vCenter Server**

  In rare occasions, if the vSphere virtual infrastructure is continuously using more than 90% of its hardware capacity, some ESXi hosts might intermittently disconnect from the vCenter Server. Connection typically restores within a few seconds.

  Workaround: If connection to vCenter Server accidentally does not restore in a few seconds, reconnect ESXi hosts manually by using vSphere Client.

- **The Utilization view of resource pools and clusters might not automatically refresh when you change the object**

  When you have already opened the **Utilization** view under the **Monitor** tab for a resource pool or a cluster and then you change the resource pool or cluster, the view might not automatically refresh. For example, when you open the **Utilization** view of one cluster and then select a different cluster, you might still see the statistics of the first cluster.

  Workaround: Click the refresh icon.

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**.

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.

vSphere Lifecycle Manager Issues

- **If you use an ESXi host deployed from a host profile with enabled stateful install as an image to deploy other ESXi hosts in a cluster, the operation fails**

  If you extract an image of an ESXi host deployed from a host profile with enabled stateful install to deploy other ESXi hosts in a vSphere Lifecycle Manager cluster, the operation fails. In the vSphere Client, you see an error such as `A general system error occurred: Failed to extract image from the host: no stored copy available for inactive VIB VMW_bootbank_xxx. Extraction of image from host xxx.eng.vmware.com failed`.

  Workaround: Use a different host from the cluster to extract an image.

- **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 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.

Guest OS Issues

- **Linux guest operating system cannot complete booting if Direct Memory Access (DMA) remapping is enabled**

  If the advanced processor setting `Enable IOMMU in this virtual machine` is enabled on a virtual machine, and the guest operating system has enabled DMA remapping, the Linux guest operating system might fail to complete the booting process. This issue affects VMs with hardware version 20 and a Linux distribution that has specific patches introduced in Linux kernel 5.18 for a VMCI feature, including but not limited to up-to-date versions of RHEL 8.7, Ubuntu 22.04 and 22.10, and SLES15 SP3, and SP4.

  Workaround: Set the advanced option `vmci.dmaDatagramSupport` to `FALSE` or disable the `Enable IOMMU in this virtual machine` option. For more information, see VMware knowledge base article 89683.

- **The guest operating system of a VM might become unresponsive due to lost communication over the Virtual Machine Communication Interface (VMCI)**

  In very specific circumstances, when a vSphere vMotion operation on a virtual machine runs in parallel with an operation that sends VMCI datagrams, services that use VMCI datagrams might see unexpected communication or loss of communication. Under the same conditions, the issue can also happen when restoring a memory snapshot, resuming a suspended VM or using CPU Hot Add. As a result, the guest operating system that depends on services communicating over VMCI might become unresponsive. The issue might also affect services

that use vSockets over VMCI. This problem does not impact VMware Tools. The issue is specific for VMs on hardware version 20 with a Linux distribution that has specific patches introduced in Linux kernel 5.18 for a VMCI feature, including but not limited to up-to-date versions of RHEL 8.7, Ubuntu 22.04 and 22.10, and SLES15 SP3, and SP4.

Workaround: Set the advanced option `vmci.dmaDatagramSupport` to `FALSE`. For more information, see VMware knowledge base article 89683.