

Versionshinweise zu VMware vSphere 8.0

VMware vSphere 8.0

ESXi 8.0

vCenter Server 8.0

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

<https://docs.vmware.com/de/>

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2023 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

- 1** Einführung 4
- 2** Neuigkeiten 5
- 3** Allgemeine Verfügbarkeit 6
- 4** Internationalisierung 7
- 5** Kompatibilität 8
- 6** Vorbereitungen 10
- 7** Installation und Upgrades für diese Version 11
- 8** Open Source-Komponenten für vSphere 8.0 15
- 9** Hinweise zu Produktunterstützung 16
- 10** Bekannte Probleme 21
 - Installations-, Upgrade- und Migrationsprobleme 21
 - Sonstige Probleme 23
 - Netzwerkprobleme 27
 - Speicherprobleme 29
 - Probleme bei vCenter Server und dem vSphere Client 30
 - VM-Verwaltungsprobleme 32
 - Probleme bei Sicherheitsfunktionen 32
 - Probleme bei vSphere Lifecycle Manager 32
 - Probleme mit VMware Host Client 33
 - Probleme mit dem Gastbetriebssystem 34

Einführung

1

VMware vSphere 8.0 | 11. Oktober 2022

ESXi 8.0 | 11. Oktober 2022 | Build 20513097

vCenter Server 8.0 | 11. Oktober 2022 | Build 20519528

Überprüfen Sie, ob Erweiterungen und Updates für diese Versionshinweise zur Verfügung stehen.

Neuigkeiten

2

- Diese Version von VMware vSphere 8.0 umfasst VMware ESXi 8.0 und VMware vCenter Server 8.0. Die neuen und erweiterten Funktionen in dieser Version sind Thema des [Blog-Beitrags mit der technischen Übersicht zu vSphere 8](#).

Die Versionshinweise zu vSphere 8.0 enthalten die folgenden Versionshinweise nicht:

- VMware vSphere with Tanzu
- Tanzu Kubernetes-Versionen
- VMware vSAN
- VMware Host Client

Allgemeine Verfügbarkeit

3

- Für vSphere 8.0 ist die allgemeine Verfügbarkeit (General Availability, GA) festgelegt. Benutzerdefinierte ISO-Images, die ESXi 8.0 GA als Basisimage verwenden und OEM-Firmware und -Treiber enthalten, sind verfügbar.

Weitere Informationen finden Sie im Blog [vSphere 8 General Availability](#).

WICHTIGER HINWEIS: Führen Sie kein Upgrade auf diese Version durch, wenn Sie den Tanzu Kubernetes Grid Service (TKG-Gastcluster) auf vSphere zusammen mit dem NSX Advanced Load Balancer (ehemals Avi Networks) verwenden und mehrere Dienstmodulgruppen konfiguriert sind. Ein Upgrade auf VMware vSphere with Tanzu 8.0 für solche Umgebungen kann dazu führen, dass keine neuen Tanzu Kubernetes-Gastcluster erstellt werden oder Upgrades vorhandener Supervisor-Cluster fehlschlagen.

Internationalisierung

4

- **VMware vSphere 8.0 ist in den folgenden Sprachen verfügbar:**
 - Englisch
 - Italienisch
 - Französisch
 - Deutsch
 - Spanisch
 - Japanisch
 - Koreanisch
 - Vereinfachtes Chinesisch
 - Traditionelles Chinesisch

Die Eingabe von Nicht-ASCII-Zeichen ist bei den Komponenten von vSphere 8.0 nicht zulässig. Hierzu zählen vCenter Server, ESXi, der vSphere Client und der VMware Host Client.

■ **Kompatibilität von virtuellen Maschinen für ESXi**

Virtuelle Maschinen, die mit ESX 3.x und höher (Hardwareversion 4) kompatibel sind, werden für ESXi 8.0 unterstützt. Virtuelle Maschinen, die mit ESX 2.x und höher (Hardwareversion 3) kompatibel sind, werden nicht unterstützt. Wenn Sie solche virtuellen Maschinen unter ESXi 8.0 verwenden möchten, führen Sie ein Upgrade der VM-Kompatibilität durch. Weitere Informationen finden Sie in der [ESXi-Upgrade-Dokumentation](#).

■ **Kompatibilität von Gastbetriebssystemen für ESXi**

Verwenden Sie die Informationen zu ESXi 8.0 im [VMware-Kompatibilitätshandbuch](#), um herauszufinden, welche Gastbetriebssysteme mit vSphere 8.0 kompatibel sind.

Die im Folgenden aufgeführten Gastbetriebssystemversionen laufen in dieser Version aus oder werden beendet. Künftige vSphere-Versionen werden diese Gastbetriebssysteme nicht mehr unterstützen:

- Windows Vista, Windows 2003/R2, Windows XP: Auslaufend
- Oracle Linux 5.x: Auslaufend
- Oracle Linux 4.9: Beendet
- CentOS 5.x: Auslaufend
- Asianux 3.0: Auslaufend
- SUSE Linux Enterprise Server 9 SP4: Beendet
- SUSE Linux Enterprise Server 10 SP4: Auslaufend
- SUSE Linux Enterprise Desktop 12: Auslaufend
- Ubuntu-Versionen 12.04, 18.10, 19.04 und 19.10: Beendet
- Debian 7.x und 8.x: Auslaufend
- Debian 6.0: Beendet
- Photon OS 1.0: Beendet
- Nicht-LTS-Versionen von Flatcar Container Linux: Beendet
- Alle OS X- und MacOS-Versionen: Beendet

- FreeBSD 9.x und 10.x: Auslaufend
- FreeBSD 7.x und 8.x: Beendet
- Solaris 10.x: Auslaufend
- Alle eComStation-Versionen: Beendet
- Alle SCO-Versionen: Beendet
- Alle CoreOS-Versionen: Beendet

- **Gerätekompatibilität für ESXi**

Verwenden Sie die Informationen zu ESXi 8.0 im [VMware-Kompatibilitätshandbuch](#), um herauszufinden, welche Geräte mit ESXi 8.0 kompatibel sind.

- **Hardwarekompatibilität für ESXi**

Um eine Liste der Prozessoren, Speichergeräte, SAN-Arrays und E/A-Geräte anzuzeigen, die mit vSphere 8.0 kompatibel sind, lesen Sie die Informationen zu ESXi 8.0 im [VMware-Kompatibilitätshandbuch](#).

- **Kompatibilität der Versionen von ESXi und vCenter Server**

Die [VMware-Produkt-Interoperabilitätsmatrix](#) liefert Details zur Kompatibilität aktueller und vorheriger Versionen von VMware vSphere-Komponenten, einschließlich ESXi, VMware vCenter Server und wahlweise anderer VMware-Produkte. Prüfen Sie die [VMware-Produkt-Interoperabilitätsmatrix](#) ebenfalls auf Informationen zu unterstützten Management- und Backup-Agents, bevor Sie ESXi oder vCenter Server installieren.

Der vSphere Lifecycle Manager und der vSphere Client befinden sich im Lieferumfang von vCenter Server.

Vorbereitungen

6

-

vSphere 8.0 erfordert eine CPU-Lizenz für bis zu 32 physische Kerne. Wenn eine CPU mehr als 32 Kerne hat, sind zusätzliche CPU-Lizenzen erforderlich, wie in [„Update to VMware’s per-CPU Pricing Model“](#) angekündigt. Vor dem Upgrade von ESXi-Hosts können Sie die Anzahl der erforderlichen Lizenzen mit dem Tool zum Zählen von Lizenzen ermitteln, das unter [„Counting CPU licenses needed under new VMware licensing policy“](#) beschrieben ist.

Installation und Upgrades für diese Version

7

■ Änderungen bei VMware Tools im Lieferumfang in ESXi 8.0

- Die folgenden VMware Tools-ISO-Images werden mit ESXi 8.0 gebündelt:

- **windows.iso:** VMware Tools 12.0.6 unterstützt Windows 7 SP1 oder Windows Server 2008 R2 SP1 und höher.
- **linux.iso:** VMware Tools 10.3.24-ISO-Image für das Linux-Betriebssystem mit `glibc` 2.11 oder höher.

Die folgenden VMware Tools-ISO-Images stehen zum Download zur Verfügung:

- VMware Tools 11.0.6:
 - **windows.iso:** für Windows Vista (SP2) und Windows Server 2008 Service Pack 2 (SP2).
- VMware Tools 10.0.12:
 - **winPreVista.iso:** für Windows 2000, Windows XP und Windows 2003.
 - **linuxPreGLibc25.iso:** unterstützt Linux-Gastbetriebssysteme vor Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04 und andere Distributionen mit einer `glibc`-Version vor 2.5.
- **solaris.iso:** VMware Tools-Image 10.3.10 für Solaris.
- **darwin.iso:** Unterstützt Mac OS X-Versionen 10.11 und höher.

Befolgen Sie die in den folgenden Dokumenten aufgeführten Vorgehensweisen, um VMware Tools für Plattformen, die nicht mit ESXi gebündelt sind, herunterzuladen:

- [Versionshinweise zu VMware Tools 12.0.6](#)
- [Frühere Versionen von VMware Tools](#)
- [Wichtige Informationen zu VMware Tools für Administratoren](#)
- [VMware Tools für Hosts, die mit Auto Deploy bereitgestellt wurden](#)
- [Aktualisieren von VMware Tools](#)

■ Installationshinweise

In der Dokumentation zur [Installation und Einrichtung von ESXi](#) und zur [Installation und Einrichtung von vCenter Server](#) finden Sie Informationen zum Installieren und Konfigurieren von ESXi und vCenter Server.

Wenngleich die Installation unkompliziert ist, sind viele der nachfolgenden Konfigurationsschritte äußerst wichtig. Lesen Sie folgende Dokumente:

„Lizenzmanagement“ in der Dokumentation [vCenter Server und Hostverwaltung](#)

„Netzwerk“ in der Dokumentation [vSphere-Netzwerk](#)

„Sicherheit“ in der Dokumentation [vSphere-Sicherheit](#) für Informationen zu Firewall-Ports

Das Tool VMware Configuration Maximums unterstützt Sie bei der Planung Ihrer vSphere-Bereitstellungen. Verwenden Sie dieses Tool, um die Grenzwerte für virtuelle Maschinen, ESXi, vCenter Server, vSAN, Netzwerk usw. anzuzeigen. Sie können damit auch die Grenzwerte von zwei oder mehr Produktversionen vergleichen. Das Tool [VMware Configuration Maximums](#) lässt sich am besten auf Geräten mit großem Bildschirm, wie etwa Desktops und Laptops, anzeigen.

- **Veraltete USB- oder SD-Kartengeräte für die vollständige ESXi-Installation:** Ab ESXi 8.0 werden ältere SD- und USB-Geräte nur noch eingeschränkt unterstützt, und die Zertifizierung neuer Plattformen mit SD-Karten wird nicht mehr unterstützt. SD- und USB-Geräte werden für Startbankpartitionen unterstützt. Sie finden eine Liste validierter Geräte auf partnerweb.vmware.com. Die Verwendung von SD- und USB-Geräten zum Speichern von ESX-OSData-Partitionen wird nicht mehr empfohlen. Die beste Vorgehensweise besteht darin, ein separates, dauerhaftes lokales Gerät mit mindestens 32 GB zum Speichern des ESX-OSData-Volumes bereitzustellen. Weitere Details finden Sie im VMware-Knowledgebase-Artikel [85685](#).
- **Erhöhte ESXi-Boot-Speicheranforderungen:** Die Mindestanforderungen an den Arbeitsspeicher für das Booten von ESXi wurden von 4 GB auf 8 GB erhöht. Die zum Ausführen von VMs erforderliche Mindestmenge an Arbeitsspeicher bleibt unverändert bei 8 GB.
- **Die Option „reboot -f“ wird für die ESXi-Installation mit einer DPU nicht unterstützt:** Obwohl ESXi die Option `-f force` für den Neustart unterstützt, kann der erzwungene Neustart einen ungültigen Status verursachen, wenn Sie `reboot -f` in einer ESXi-Konfiguration mit einer DPU verwenden.
- ESXi kann nicht mithilfe von Auto Deploy auf DPUs installiert werden. Für Neuinstallationen von ESXi auf DPU stehen Ihnen die interaktive und die skriptgesteuerte Methode zur Verfügung.

■ Upgrades und Installationen nicht zulässig für nicht unterstützte CPUs

- Achten Sie bei ESXi-Hosts, die Broadcom `bnxtnet` NIC-Treiber verwenden, vor der Installation von ESXi 8.0 oder einem entsprechenden Upgrade darauf, dass die NIC-Firmware eine kompatible Version aufweist, etwa 222.1.68.0 oder höher. Wenn Sie keine kompatible Firmware-Version gemäß Angabe im [VMware Compatibility Guide](#) oder entsprechend der Empfehlung des OEM verwenden, kann es zu Problemen wie Leistungseinbußen, Firmware-Fehlern oder ESXi-Host-Ausfällen kommen.
- vSphere 8.0 unterstützt keine CPUs mehr, die von den Hardwareanbietern als „Ende der Unterstützung“ oder „Ende der Lebensdauer“ gekennzeichnet wurden. Weitere Details finden Sie im VMware-Knowledgebase-Artikel [82794](#).
- **Veraltete BIOS-Version:** In vSphere 8.0 wird das Starten von ESXi-Hosts mit der Unified Extensible Firmware Interface (UEFI) dringend empfohlen. Einige ESXi 8.0-Hosts werden im Legacy-BIOS-Modus möglicherweise nicht erfolgreich gestartet. Wenn sich diese Änderung auf Ihr vSphere-System auswirkt, finden Sie Details und Aktionspläne in den VMware-Knowledgebase-Artikeln [84233](#) und [89682](#).

■ Upgrade-Hinweise

- Bei Upgrades von vSphere-Systemen ist Best Practice, dass die vCenter-Version immer größer oder gleich der ESXi-Version ist. Damit wird dafür gesorgt, dass Sie alle neuen Funktionen nutzen können, die mit der neuesten vSphere-Version eingeführt wurden. Weitere Informationen zu vSphere-Build-Nummern finden Sie unter [Build-Nummern und Versionen von VMware vCenter Server](#) sowie unter [Build-Nummern und Versionen von VMware ESXi/ESX](#). Informationen zu den Upgrade-Einschränkungen für vSphere Back-in-Time-Versionen finden Sie im VMware-Knowledgebase-Artikel [67077](#).
- Vor dem Upgrade von vCenter im Enhanced Link Mode (ELM) empfiehlt es sich, ausgeschaltete gleichzeitige Snapshots für alle vCenter Server und Platform Services Controller innerhalb der Single Sign-On-Domäne zu erstellen, um Synchronisierungsprobleme bei der Replizierung zu vermeiden. Wenn ein Rollback auf einen Snapshot erforderlich ist, können alle PSC- und vCenter Server auf den vorherigen Zustand zurückgesetzt werden.
- vSphere 8.0 ist nicht mit VMware NSX for vSphere (NSX-V) kompatibel. Upgrades auf vSphere 8.0 von Systemen mit NSX for vSphere werden nicht unterstützt. Weitere Informationen finden Sie im [NSX-Migrationshandbuch](#).
- Ein direktes Upgrade von ESXi 6.5 auf 8.0 wird nicht unterstützt, da die mit ESXi 6.5 eingeführte Version 2.4 von VMKAPI aus ESXi 8.0 entfernt wurde. Wenn Sie ESXi 6.5-VIBs haben, die von VMKAPI Version 2.4 in einer 6.7.x- oder 7.x-Umgebung abhängen, verhindern diese VIBs ein Upgrade von 6.7.x oder 7.x auf 8.0. In dem für das Upgrade auf ESXi 8.0 verwendeten Image dürfen Sie nur VIBs der Version 6.7.x oder höher verwenden. Um neuere Versionen der VIBs bereitzustellen, können Sie sich mit dem entsprechenden Development Kit für Versionen von VMKAPI ab 2.4 neu zertifizieren. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [88646](#).

- Wenn Sie ein Upgrade auf ESXi 8.0 von einem Host mit einem vom Treiber `nmlx4_en` unterstützten Gerät oder einem im Treiber `lpfc` entfernten Gerät durchführen, sind diese nicht behebbaren Folgen möglich: Verlust des Zugriffs auf Speicher oder Datenspeicher, Verlust des Netzwerkzugriffs sowie Verlust der vorherigen Konfiguration auf dem Host. Vor dem Upgrade auf ESXi 8.0 sollten Sie Geräte ersetzen, die zuvor vom Treiber `nmlx4_en` unterstützt wurden, oder Geräte, die im Treiber `lpfc` der Version 8.0 entfernt wurden. Eine vollständige Liste der Geräte, die in ESXi 8.0 nicht mehr unterstützt werden, finden Sie im VMware-Knowledgebase-Artikel [88172](#).
- Die Installations- und Upgrade-Workflows von ESXi 8.0 blockieren VIBs, die keine SHA256-Prüfsumme in ihren Metadaten aufweisen, z. B. VIBs von ESXi-Versionen vor 6.7. Sie müssen solche VIBs durch neuere Versionen ersetzen: 6.7.x, 7.x und 8.0.
- Ein ESXi-Upgrade auf DPUs wird bei der interaktiven oder skriptgesteuerten Methode nicht unterstützt. Sie können stattdessen vSphere Lifecycle Manager oder ESXCLI verwenden. So löst beispielsweise ein auf einem ESXi-Host ausgeführter Befehl `esxcli software *` automatisch den gleichen Vorgang auf der DPU aus, wenn diese auf dem Host vorhanden ist.

Open Source-Komponenten für vSphere 8.0



Nach der Anmeldung bei Ihrem [Customer Connect](#)-Konto finden Sie Informationen über Copyright und Lizenzen für die in vSphere 8.0 enthaltenen Open Source-Softwarekomponenten unter https://customerconnect.vmware.com/de/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/8_0#open_source. Auf der Registerkarte **Open Source** können Sie auch die Quelldateien für jede GPL-, LGPL- oder vergleichbare Lizenz herunterladen, die die Verfügbarkeit des Quellcodes bzw. dessen Modifizierung für die jeweils neueste vorliegende vSphere-Version erfordert.

Hinweise zu Produktunterstützung

9

■

- **Unterstützung der Datenverarbeitungseinheit (DPU):** vSphere 8.0 unterstützt in ESXi NVIDIA- und AMD Pensando SmartNIC-Geräte, die auch als DPUs bezeichnet werden. Weitere Informationen finden Sie unter [Einführung in VMware vSphere® Distributed Services Engine™](#) und [Netzwerkbeschleunigung durch DPUs](#).
- **TPM-Bereitstellungsrichtlinie:** Ab ESX 8.0 können Sie die TPM-Bereitstellungsrichtlinie verwenden, mit der virtuelle TPM-Geräte während Klon- oder Bereitstellungsvorgängen automatisch ersetzt werden können. Weitere Informationen finden Sie unter [Windows 11 Support on vSphere](#).
- **Veraltete N-Port-ID-Virtualisierung (NPIV):** NPIV ist ein ANSI T11-Standard, der definiert, wie ein einzelner Fibre Channel-HBA-Port mithilfe mehrerer WWPNs (Worldwide Port Names) beim Fabric registriert wird. NPIV ist aufgrund vieler vorhandener Alternativen in einer zukünftigen Version von vSphere veraltet.
- **Veraltete integrierte Windows-Authentifizierung (IWA):** Aufgrund von Leistungsproblemen bei der IWA-basierten Authentifizierung wird die Verwendung von IWA in vSphere 8.0 eingestellt. Sie können AD über LDAP oder ADFS verwenden.
- **Common Information Model (CIM) und Service Location Protocol (SLP) werden als veraltet eingestuft:** Die Unterstützung für CIM und SLP ist in ESXi 8.0 aufgrund von Sicherheitsproblemen veraltet und wird in einer zukünftigen ESXi-Version entfernt. Alternativ können Sie das Daemon Software Development Kit (DSDK) für Lösungen verwenden, die CIM verwenden, wie z. B. das CIM Provider Development Kit (CIMPDK) und das VAIO Development Kit (vSphere APIs für die E/A-Filterung). Es ist kein CIMPDK für vSphere 8.0 freigegeben, aber CIM-Anbieter für ESXi 7.x. funktionieren weiterhin auf ESXi 8.0, um einen reibungslosen Upgrade-Vorgang zu gewährleisten.
- **Die gegenseitige Smartcard-Authentifizierung wird auf Port 3128 verschoben:** vCenter Server 8.0 verschiebt die gegenseitige Smartcard-Authentifizierung auf Port 3128 und erfordert einen Neustart des Security Token Service (STS) während der Konfiguration. Weitere Informationen finden Sie unter [Konfigurieren des Reverse-Proxys zum Anfordern von Clientzertifikaten](#).
- Der VMware Inbox `qedentv` NIC-Treiber von Marvell unterstützt NVMe/TCP in ESXi 8.0 nicht im ENS (Enhanced Networking Stack)-Modus.

- **Veraltete vSphere Lifecycle Manager-Baselines:** Die Verwaltung von Clustern mit vSphere Lifecycle Manager-Baselines und -Baselinegruppen (Legacy-Workflows von vSphere Update Manager) wird in vSphere 8.0 unterstützt, die Unterstützung wird jedoch in einer zukünftigen vSphere-Version eingestellt. Anstelle von Baselines und Baselinegruppen können Sie mithilfe von vSphere Lifecycle Manager-Images Aufgaben auf Clusterebene ausführen, wie z. B. die Installation einer gewünschten ESXi-Version auf allen Hosts in einem Cluster, die Installation und Aktualisierung von Drittanbietersoftware, die Aktualisierung und das Upgrade von ESXi oder Firmware, die Erstellung von Empfehlungen und die Verwendung eines empfohlenen Images für Ihren Cluster. Weitere Informationen finden Sie im Blog [Introducing vSphere Lifecycle Management \(vLCM\)](#).
- **Beschränkung vordefinierter vSphere Lifecycle Manager-Baselines auf VMware-Inhalte:** Ab vSphere 8.0 sind vordefinierte vSphere Lifecycle Manager-Baselines ausschließlich auf von VMware bereitgestellten Inhalt beschränkt. Inhalte von Drittanbietern, wie z. B. asynchrone Treiber und Tools, können nicht mehr Teil vordefinierter Baselines sein. Wenn zur Aktualisierung von Baselines Drittanbieterinhalte hinzugefügt werden müssen, müssen benutzerdefinierte Baselines manuell erstellt werden.
- **Veraltete Patch Manager-APIs:** Mit vSphere 8.0 sind Patch Manager-APIs veraltet. Patch Manager-APIs werden in vSphere 8.0 unterstützt, aber die Unterstützung wird in einer zukünftigen Version von vSphere eingestellt. Anstelle der Patch Manager-APIs können Sie die neuesten vSphere APIs verwenden, die im [Referenzhandbuch zur vSphere-API-Automatisierung](#) dokumentiert sind.
- **Veraltete lokale Plug-Ins:** Durch die Umstellung der vSphere-Plug-Ins auf eine Remote-Plug-In-Architektur ist in vSphere 8.0 die Unterstützung für lokale Plug-Ins veraltet. VMware plant, die Unterstützung für lokale Plug-Ins in einer zukünftigen vSphere-Version einzustellen. Weitere Informationen finden Sie im Blog [Deprecating the Local Plugins :- The Next Step in vSphere Client Extensibility Evolution](#) und im VMware-Knowledgebase-Artikel [87880](#).
- **Aufhebung der Unterstützung für 32-Bit-Benutzerwelten:** ESXi 8.0 unterstützt keine 32-Bit-Benutzerwelten und Sie müssen jede Lösung, die das 32-Bit-Subsystem verwendet, neu kompilieren.
- **Entfernen von VMKAPI v2.4:** vSphere 8.0 unterstützt VMKAPI v2.4 nicht. Sie müssen neuere Versionen der API verwenden und sich mit dem neuesten Development Kit neu zertifizieren.
- **Entfernen des Treibers nmlx4_en:** ESXi 8.0 entfernt den Treiber `nmlx4_en` und alle Geräte für diesen Treiber werden nicht mehr unterstützt.
- **Entfernen von Trusted Platform Module (TPM) 1.2:** VMware stellt die Unterstützung von TPM 1.2 und zugehörigen Funktionen wie TPM 1.2 mit TXT ein. Um die vSphere-Funktionen vollständig nutzen zu können, können Sie TPM 2.0 anstelle von TPM 1.2 verwenden.

- **Entfernen unsicherer Verschlüsselungen:** X.509-Zertifikate, die einen SHA-1-Signaturalgorithmus oder andere schwache Signaturalgorithmen angeben, werden in vSphere 8.0 nicht mehr unterstützt. Vorabprüfungen verhindern ein Upgrade auf vCenter Server 8.0 und ESXi 8.0, wenn Zertifikate mit einem schwachen Signaturalgorithmus verwendet werden. Die Wartungsschritte sind im VMware-Knowledgebase-Artikel [89424](#) beschrieben.
- **Entfernen von Software-FCoE-Adaptern:** In vSphere 8.0 wird die Option zum Konfigurieren von Software-FCoE-Adaptern, die den nativen FCoE-Stack in ESXi verwenden, entfernt und nicht mehr unterstützt. Diese Änderung hat keine Auswirkungen auf Hardware-FCoE-Adapter und -Treiber.
- **Einstellung der Unterstützung für E/A-Geräte, die von den Treibern nmlx4_en und lpfc verwendet werden:** VMware beabsichtigt, die Unterstützung für E/A-Geräte einzustellen, die das EOL erreichen, z. B. Geräte, die zuvor vom Treiber `lpfc` unterstützt wurden, sowie alle Geräte für den Treiber `nmlx4_en`. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [88172](#).
- **Sie können eine schreibgeschützte VMDK nicht als FCD registrieren:** In vSphere 8.0 wird eine Virtual Storage Lifecycle Management-API, die auf einer als FCD registrierten schreibgeschützten VMDK aufgerufen wird, nicht unterstützt.
- **Einstellung der Unterstützung für Gastbetriebssysteme:** vSphere 8.0 stellt die Unterstützung für die folgenden Gastbetriebssysteme ein:
 - eComStation
 - SCO Openserver
 - SCO Unixware
 - Oracle Linux 4.x
 - SLES9 SP4
 - Ubuntu 12.04 LTS
 - Debian 6.0
 - FreeBSD 7.x
 - FreeBSD 8.x
- **Verhindern der Ausführung nicht vertrauenswürdiger Binärdateien:** Ab ESXi 8.0 wurde eine neue Sicherheitsoption standardmäßig aktiviert, um die Ausführung nicht vertrauenswürdiger Binärdateien einzuschränken und so besser vor Ransomware-Angriffen zu schützen. Die Option `execInstalledOnly` ist jetzt ein Laufzeitparameter, der die Ausführung von Binärdateien wie Anwendungen und vmkernel-Modulen einschränkt, um die Sicherheit zu verbessern und vor Verstößen und Kompromittierungen zu schützen. Wenn `execInstalledOnly` aktiviert ist, können nur Binärdateien ausgeführt werden, die lokal über eine VIB installiert wurden.

- **Unterstützung für OpenSSL 3.0:** ESXi 8.0 unterstützt OpenSSL 3.0; die Unterstützung für TLS 1.0 und TLS 1.1 entfällt. OpenSSL 3.0 wird von vCenter nicht unterstützt. In vCenter ist TLS 1.2 standardmäßig aktiviert und TLS 1.0 und TLS 1.1 sind standardmäßig deaktiviert, können aber vorübergehend aktiviert werden.
- **Hardware-Zeitstempel-basierte PTP-Zertifizierung (Precision Time Protocol) für NICs:** vSphere 8.0 fügt eine Zertifizierung für NICs hinzu, die Hardware-Zeitstempel-basiertes PTP als Teil des IOVP-Zertifizierungsprogramms (I/O Vendor Partner) unterstützen.
- **NVMe over Fabrics (NVMe-oF)-Unterstützung für vSphere Virtual Volumes:** vSphere 8.0 fügt NVMe-oF-Unterstützung für vSphere Virtual Volumes im Rahmen des IOVP NVMe-FC Zertifizierungsprogramms hinzu.
- **Skalierungsverbesserungen bei NVMeoF-RDMA:** Mit NVMeoF können Sie NVMe-Namespaces und -Pfade in vSphere 8.0 auf 256 bzw. 4.000 skalieren.
- **Erweiterte NVMe-oF Discovery Service-Unterstützung:** vSphere 8.0 fügt die dynamische Erkennung von Geräten für konforme NVMe Discovery Services und Speicher-Arrays hinzu.
- **Syslog-Verbesserungen:** In vSphere 8.0 wird das Format der Protokolle des ESXi-Syslog-Daemons für alle vSphere- und VCF-Produkte vereinheitlicht. Wenn Syslog-Protokolldateien vom System direkt aus ESXi verwendet werden, müssen Sie Ihre Lösungen aktualisieren. Weitere Informationen finden Sie unter [Konfigurieren der Systemprotokollierung](#). Sie können Übertragungen von Syslog-Meldungen aus ESXi in Übereinstimmung mit RFC 5424- oder Frame-Meldungen optional konfigurieren. Weitere Informationen finden Sie unter [Protokolle, Formate und Rahmen von ESXi Syslog-Meldungen](#). Sie können alle Syslog-Steuerungsparameter entweder mithilfe des vSphere Client oder des VMware Host Client festlegen und müssen SSH oder ESXCLI nicht verwenden.
- **Auslaufende LSI SAS-Controller:** vSphere 8.0 kann den LSI SAS-Controller für VMs unter Windows 10 und höher oder Windows Server 2016 und höher automatisch und sicher durch den nativen VMware PVSCI-Controller ersetzen, da der LSI SAS-Treiber für Windows das Ende seiner Lebensdauer erreicht hat. Für VMs unter Versionen vor Windows 10 und Windows Server 2016 können Sie den LSI SAS-Controller manuell durch PVSCI, SATA oder einen NVMe-Controller ersetzen.
- **Konformität der Standard-RSA-Schlüssellänge mit Impact Level 6 (IL-6) des U.S.-Verteidigungsministeriums:** Um den IL6-Standards zu entsprechen, erhöht sich die standardmäßige RSA-Schlüssellänge, die für vCenter Server-Zertifikate generiert wird, in vSphere 8.0 von 2048 Bit auf 3072 Bit.
- **Verwalten des Benutzerzugriffs auf ESXi Shell:** Ab vSphere 8.0 können Benutzer mit der Administratorrolle den ESXi Shell-Zugriff auf Benutzerkonten entfernen oder gewähren. Weitere Informationen finden Sie unter [Vorgehensweise zum Konfigurieren eines vSphere-Hostprofils für die Sicherheit](#).

- **Einstellung der Unterstützung für Apple Mac-Plattformen:** ESXi 8.0 unterstützt nicht länger die Plattformen Apple MacPro und Apple MacMini sowie macOS als Gastbetriebssystem. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [88698](#).
- **Virtuelle Hardwareversion 20:** ESXi 8.0 führt die virtuelle Hardware Version 20 ein, um die Unterstützung für virtuelle Maschinen mit höheren Maximalwerten für Ressourcen zu aktivieren, und:
 - Virtuelle NUMA-Topologie
 - Verbesserte Direct Path I/O
 - Virtuelles Hyper-Threading
 - vMotion App-Benachrichtigung
 - VM-DataSets
 - OpenGL 4.3
 - UEFI 2.7A
- **Verbesserte Skalierbarkeit mit vSphere Lifecycle Manager:** Mit vSphere 8.0 erhöht sich die Skalierbarkeit für Vorgänge mit vSphere Lifecycle Manager-Images von 280 auf 1.000 ESXi-Hosts.
- **Unterstützung für UEFI 2.7A:** vSphere 8.0 entspricht der UEFI-Spezifikation Version 2.7A zur Unterstützung einiger Funktionen von Microsoft Windows 11.
- **vSphere Configuration Profiles :** vSphere 8.0 startet vSphere Configuration Profiles in der Tech-Vorschau. Diese Funktion ermöglicht Ihnen die Verwaltung von ESXi-Clusterkonfigurationen durch Angabe einer gewünschten Hostkonfiguration auf Clusterebene, automatisiert die Prüfung von ESXi-Hosts auf Übereinstimmung mit der angegebenen gewünschten Konfiguration und standardisiert alle Hosts, die nicht konform sind. Der Start der Tech-Vorschau gilt nur für Kunden die Standard-Switches verwenden. VMware vSphere Distributed Switch (VDS) wird nicht unterstützt und erfordert die Verwendung von vSphere Lifecycle Manager-Images für das Management Ihrer Cluster.
- **Entfernen von RDMA-over-Converged-Ethernet (RoCE) v1:** Ab vSphere 8.0 unterstützt VMware das Netzwerkprotokoll RoCE v1 nicht mehr. Sie können RoCEv2 verwenden. Stellen Sie sicher, dass Sie Netzwerkadapter für paravirtualisierten direkten Remotespeicherzugriff (Paravirtualized Remote Direct Memory Access, PVRDMA) für virtuelle Maschinen und Gastbetriebssysteme auf einen Adapter migrieren, der RoCEv2 unterstützt.

Bekannte Probleme

10

Dieses Kapitel enthält die folgenden Themen:

- Installations-, Upgrade- und Migrationsprobleme
- Sonstige Probleme
- Netzwerkprobleme
- Speicherprobleme
- Probleme bei vCenter Server und dem vSphere Client
- VM-Verwaltungsprobleme
- Probleme bei Sicherheitsfunktionen
- Probleme bei vSphere Lifecycle Manager
- Probleme mit VMware Host Client
- Probleme mit dem Gastbetriebssystem

Installations-, Upgrade- und Migrationsprobleme

- **Zweite Phase des Wiederherstellungsvorgangs von vCenter Server friert bei 90 % ein**

Wenn Sie das GUI-Installationsprogramm von vCenter Server oder die vCenter Server Appliance Management Interface (VAMI) verwenden, um ein vCenter aus einem dateibasierten Backup wiederherzustellen, bleibt der Wiederherstellungsworkflow unter Umständen bei 90 % mit der Fehlermeldung `401 Unable to authenticate user` stehen, obwohl die Aufgabe im Back-End erfolgreich abgeschlossen wird. Das Problem tritt auf, wenn der eingesetzte Rechner auf eine andere Zeit eingestellt ist als der NTP-Server, sodass eine Zeitsynchronisierung erforderlich ist. Infolge der Zeitsynchronisierung kann die laufende Sitzung der GUI oder VAMI durch eine Taktverschiebung gestört werden.

Problemumgehung: Wenn Sie das GUI-Installationsprogramm verwenden, können Sie den Wiederherstellungsstatus mit dem Befehl `restore.job.get` in der Shell `appliancecli` abrufen. Wenn Sie die VAMI verwenden, aktualisieren Sie Ihren Browser.

- **Nach dem Upgrade auf ESXi 8.0 gehen aufgrund veralteter Parameter möglicherweise einige Einstellungen des Treibermoduls `nmlx5_core` verloren**

Einige Modulparameter für den Treiber `nmlx5_core`, beispielsweise `device_rss`, `drss` und `rss`, sind in ESXi 8.0 veraltet, und alle von den Standardwerten abweichenden benutzerdefinierten Werte werden nach einem Upgrade auf ESXi 8.0 verworfen.

Problemumgehung: Ersetzen Sie die Werte der Parameter `device_rss`, `drss` und `rss` wie folgt:

- `device_rss`: Verwenden Sie den Parameter `DRSS`
- `drss`: Verwenden Sie den Parameter `DRSS`
- `rss`: Verwenden Sie den Parameter `RSS`
- **Wenn während des Upgrades auf ESXi 8.0 ein vCenter Server Security Token Service (STS) aktualisiert wird, kommt es beim Upgrade unter Umständen zu einem Fehler**

In vSphere 8.0 wird ein von VMCA erstelltes STS-Signaturzertifikat automatisch durch vCenter Single Sign-On verlängert. Die automatische Verlängerung erfolgt, bevor das STS-Signaturzertifikat abläuft und bevor der 90-Tage-Ablaufalarm ausgelöst wird. Bei langwierigen Upgrade- oder Wartungsaufgaben unter Verwendung eines vSphere Lifecycle Manager-Images auf mehreren ESXi-Hosts in einem Cluster legt vSphere Lifecycle Manager jedoch eventuell intern einen Cache mit STS-Zertifikaten an. In sehr seltenen Fällen kann, wenn eine Aufgabe zur Aktualisierung von STS-Zertifikaten parallel zu einer langwierigen Upgrade- oder Wartungsaufgabe startet, die Upgrade-Aufgabe fehlschlagen, da sich die STS-Zertifikate im internen Cache eventuell von den aktualisierten Zertifikaten unterscheiden. Nach dem Fehlschlagen der Upgrade-Aufgabe verbleiben einige ESXi-Hosts möglicherweise im Wartungsmodus.

Problemumgehung: Beenden Sie manuell alle ESXi-Hosts im Wartungsmodus und beginnen Sie erneut mit dem Upgrade beziehungsweise der Wartung. Das Aktualisieren oder Importieren und Ersetzen der STS-Signaturzertifikate erfolgt automatisch. Um Ausfallzeiten zu vermeiden, ist ein Neustart von vCenter Server dafür nicht erforderlich.

- **VMNICs können nach einem Upgrade auf ESXi 8.0 ausfallen**

Wenn der physische Peer-Switch einer VMNIC die automatische Medienerkennung nicht unterstützt oder die automatische Medienerkennung deaktiviert ist und der VMNIC-Link heruntergefahren und dann wieder hochgefahren wird, bleibt der Link nach dem Upgrade auf oder der Installation von ESXi 8.0 heruntergefahren.

Problemumgehung: Verwenden Sie eine der folgenden beiden Optionen:

- a Aktivieren Sie die Option `media-auto-detect` in den BIOS-Einstellungen, indem Sie zum System-Setup-Hauptmenü navigieren, in der Regel durch Drücken von **F2** oder Öffnen einer virtuellen Konsole. Dort gehen Sie dann zu **Geräteeinstellungen** > *<spezifisches Broadcom NIC>* > **Gerätekonfigurationsmenü** > **Automatische Medienerkennung**. Starten Sie den Host neu.
- b Alternativ dazu können Sie einen ESXCLI-Befehl ähnlich dem folgenden verwenden:
`esxcli network nic set -S <your speed> -D full -n <your nic>`. Mit dieser Option legen Sie auch eine feste Geschwindigkeit für den Link fest, und es ist kein Neustart erforderlich.

- **Sie können ESXi-Hosts der Version 8.0 nicht als Referenzhost für vorhandene Hostprofile früherer ESXi-Versionen verwenden**

Die Validierung vorhandener Hostprofile für ESXi-Versionen 7.x, 6.7.x und 6.5.x schlägt fehl, wenn nur ein 8.0-Referenzhost in der Bestandsliste verfügbar ist.

Problemumgehung: Stellen Sie sicher, dass Sie über einen Referenzhost der entsprechenden Version in der Bestandsliste verfügen. Verwenden Sie zum Beispiel einen ESXi 7.0 Update 2-Referenzhost, um ein ESXi 7.0 Update 2-Hostprofil zu aktualisieren oder zu bearbeiten.

- **Wenn Sie ein Hostprofil mit einer Software-FCoE-Konfiguration auf einen ESXi 8.0-Host anwenden, schlägt der Vorgang mit einem Validierungsfehler fehl**

Ab vSphere 7.0 ist Software-FCoE veraltet, und in vSphere 8.0 werden Software-FCoE-Profile nicht unterstützt. Wenn Sie versuchen, ein Hostprofil aus einer früheren Version auf einen ESXi 8.0-Host anzuwenden, z. B. um die Hostanpassung zu bearbeiten, schlägt der Vorgang fehl. Im vSphere Client wird ein Fehler ähnlich dem folgenden angezeigt: `Host Customizations validation error.`

Problemumgehung: Deaktivieren Sie das Unterprofil Software FCoE-Konfiguration im Hostprofil.

Sonstige Probleme

- **Das Zurücksetzen oder Wiederherstellen der ESXi-Systemkonfiguration in einem vSphere-System mit DPUs kann zu einem ungültigen Status der DPUs führen**

Wenn Sie die ESXi-Systemkonfiguration in einem vSphere-System mit DPUs zurücksetzen oder wiederherstellen, z. B. durch Auswahl von **Systemkonfiguration zurücksetzen** in der direkten Konsole, kann der Vorgang zu einem ungültigen Zustand der DPUs führen. In der DCUI sehen Sie möglicherweise Fehler wie `Failed to reset system configuration. Note that this operation cannot be performed when a managed DPU is present.` Ein Backend-Aufruf der Option `-f` zum Erzwingen eines Neustarts wird für ESXi-Installationen mit einer DPU nicht unterstützt. Obwohl ESXi 8.0 die Option `-f` zum Erzwingen eines Neustarts unterstützt, kann der erzwungene Neustart einen ungültigen Status verursachen, wenn Sie `reboot -f` in einer ESXi-Konfiguration mit einer DPU verwenden.

Problemumgehung: Installieren Sie ESXi neu. Vermeiden Sie das Zurücksetzen der ESXi-Systemkonfiguration in einem vSphere-System mit DPUs.

- **Im vSphere API-Explorer, in der VMware Datacenter CLI (DCLI) und in PowerCLI wird die API-Option „contentinternal“ angezeigt, die nicht funktionsfähig ist**

Die API-Option **contentinternal** wird in den Metadaten von vSphere API Explorer, DCLI und PowerCLI angezeigt. Wenn Sie beispielsweise `https://<your vCenter IP>/ui/app/devcenter/api-explorer` öffnen, wird die Option im Dropdown-Menü **API auswählen** angezeigt. Diese Option ist nicht funktionsfähig.

Problemumgehung: Ignorieren Sie die API-Option **contentinternal** und verwenden Sie sie nicht.

- **Wenn Sie eine VM mit einer früheren HW-Version als 20 mit einer Anbietergerätegruppe konfigurieren, funktionieren diese VMs möglicherweise nicht wie erwartet**

Anbietergerätegruppen, die die Bindung von Hochgeschwindigkeits-Netzwerkgeräten und der GPU ermöglichen, werden nur auf VMs mit HW-Version 20 und höher unterstützt. Sie werden jedoch nicht daran gehindert, eine VM mit einer HW-Version vor 20 mit einer Anbietergerätegruppe zu konfigurieren. Solche VMs funktionieren möglicherweise nicht wie erwartet: So schlägt beispielsweise das Einschalten fehl.

Problemumgehung: Stellen Sie sicher, dass die VM HW-Version 20 ist, bevor Sie eine Anbietergerätegruppe in dieser VM konfigurieren.

- **Wenn Sie eine virtuelle Maschine aus einer OVF-Datei oder aus der Inhaltsbibliothek bereitstellen, wird die Anzahl der Kerne pro Socket für die VM auf 1 festgelegt**

Wenn Sie eine virtuelle Maschine aus einer OVF-Datei oder aus der Inhaltsbibliothek bereitstellen, wird die Anzahl der Kerne pro Socket nicht automatisch von ESXi ausgewählt, sondern auf 1 festgelegt.

Problemumgehung: Sie können die Anzahl der Kerne pro Socket mithilfe des vSphere-Clients manuell festlegen.

- **Sie können ein PCI-Passthrough-Gerät, das einem virtuellen NUMA-Knoten (Non-Uniform Memory Access) zugewiesen ist, nicht aus einer virtuellen Maschine entfernen, bei der das Hinzufügen von CPUs im laufenden Betrieb aktiviert ist**

Obwohl bei aktivierter CPU-Hot-Add-Funktion das Hinzufügen von vCPUs zu einer laufenden virtuellen Maschine standardmäßig aktiviert ist, wird die virtuelle NUMA-Topologie deaktiviert. Wenn Sie jedoch einem NUMA-Knoten ein PCI-Passthrough-Gerät zugewiesen haben, enden Versuche, das Geräte zu entfernen, mit einem Fehler. Im vSphere Client sehen Sie Meldungen wie beispielsweise `Invalid virtual machine configuration. Virtual NUMA cannot be configured when CPU hotadd is enabled.`

Problemumgehung: Keine.

- **In der Virtual Appliance Management Interface (VAMI) wird in der Phase vor dem Upgrade eine Warnung angezeigt**

Durch die Umstellung der vSphere-Plug-Ins auf eine Remote-Plug-In-Architektur ist in vSphere 8.0 die Unterstützung für lokale Plug-Ins veraltet. Wenn in Ihrer vSphere 8.0-Umgebung lokale Plug-Ins vorhanden sind, können einige Änderungen an diesen Plug-Ins dazu führen, dass die vor dem Upgrade per VAMI durchgeführte Prüfung scheitert.

In der Ergebnisanzeige zu der dem Update vorausgehenden Prüfung wird eine Fehlermeldung ähnlich der folgenden angezeigt:

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.

Problemumgehung: Weitere Informationen finden Sie im [VMware Compatibility Guide](#) und in der [VMware Product Interoperability Matrix](#). Alternativ können Sie sich vor den weiteren Upgrade-Schritten bei den Plug-In-Anbietern nach Empfehlungen erkundigen, um sicherzugehen, dass die lokalen Plug-Ins in Ihrer Umgebung mit vCenter Server 8.0 kompatibel sind. Weitere Informationen finden Sie im Blog [Deprecating the Local Plugins :- The Next Step in vSphere Client Extensibility Evolution](#) und im VMware-Knowledgebase-Artikel [87880](#).

- **Einige Uplinks des ionic_en-Treibers funktionieren möglicherweise nur mit einer einzigen Empfangswarteschlange und es tritt eine Leistungsbeeinträchtigung im nativen Modus ein**

Pensando DSC-Adapter (Distributed Services Platform) bieten zwei Hochgeschwindigkeits-Ethernet-Controller (beispielsweise `vmnic6` und `vmnic7`) sowie einen Management-Controller (beispielsweise `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

```

Die Hochgeschwindigkeits-Ethernet-Controller `vmnic6` und `vmnic7` werden zuerst registriert; ihr Betrieb erfolgt mit RSS-Einstellung auf 16 Empfangswarteschlangen.

```

:~] 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 }

```

In seltenen Fällen kann es allerdings vorkommen, dass bei einer zuerst erfolgreichen Registrierung des Management-Controllers `vmnic8` beim vSphere Distributed Switch der Uplink des Hochgeschwindigkeits-Ethernet-Controllers `vmnic6` oder `vmnic7` mit RSS-Einstellung auf 1 Empfangswarteschlange betrieben wird.~] `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 }`

Infolgedessen kann es zu einer Leistungsbeeinträchtigung im nativen Modus kommen.

Problemumgehung: Laden Sie den `ionic_en` driver auf ESXi mit den folgenden Befehlen neu::~] `esxcfg-module -u ionic_en::~] esxcfg-module ionic_en::~] localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal bind.`

- **Wenn eine NVIDIA BlueField-DPU im Hardware-Offload-Modus deaktiviert ist, können virtuelle Maschinen mit konfigurierter virtueller SR-IOV-Funktion nicht eingeschaltet werden**

NVIDIA BlueField-DPUs müssen im Hardware-Offload-Modus aktiviert sein, damit virtuelle Maschinen mit konfigurierter virtueller SR-IOV-Funktion eingeschaltet und betrieben werden können.

Problemumgehung: Verwenden Sie immer den standardmäßigen Hardware-Offload-Modus, der für NVIDIA BlueField-DPUs aktiviert ist, wenn Sie VMs mit konfigurierter virtueller SR-IOV-Funktion an einen virtuellen Switch angeschlossen haben.

- **Wenn Sie in einer Remotemanagementanwendung, die Sie zur Installation von ESXi 8.0 verwenden, eine USB-Schnittstelle aktiviert haben, sehen Sie einen zusätzlichen Standard-Switch vSwitchBMC mit Uplink vusb0**

Ab vSphere 8.0 wird sowohl bei Integrated Dell Remote Access Controller (iDRAC) als auch bei HP Integrated Lights Out (ILO) mit aktivierter USB-Schnittstelle (vUSB bzw. vNIC) ein zusätzlicher Standard-Switch `vSwitchBMC` mit Uplink `vusb0` auf dem ESXi-Host erstellt. Auf einigen Servern ist dies angesichts der Einführung von Datenverarbeitungseinheiten (Data Processing Units, DPUs) zu erwarten; es kann dadurch allerdings zum Fehlschlagen des Bring-Up-Prozesses der VMware Cloud Foundation kommen.

Problemumgehung: Deaktivieren Sie vor der Installation von vSphere 8.0 die USB-Schnittstelle in der von Ihnen verwendeten Remotemanagementanwendung. Richten Sie sich dazu nach der Dokumentation des Herstellers.

Verwenden Sie nach der Installation von vSphere 8.0 den ESXCLI-Befehl `esxcfg-advcfg -s 0 /Net/BMCNetworkEnable`, um die Erstellung eines virtuellen Switches `vSwitchBMC` und zugehöriger Portgruppen beim nächsten Neustart des Hosts zu verhindern.

Hier ein Skript als Beispiel:

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

Der Wert von `BMCNetworkEnable` ist 0, und der Dienst ist deaktiviert.

~# reboot

Beim Neustart des Hosts werden in Verbindung mit dem Netzwerk der Remotemanagementanwendung kein virtueller Switch, keine Portgruppe und keine VMKNIC im Host erstellt.

- **Beim Neustart eines ESXi-Hosts auf einem HPE-Server mit vorinstallierter Pensando-DPU kann es zu einer 10-minütigen Verzögerung kommen**

In seltenen Fällen kann der Neustart von HPE-Servern mit vorinstallierter Pensando-DPU mehr als 10 Minuten dauern, wenn bei der DPU ein Fehler vorliegt. Infolgedessen fallen unter Umständen ESXi-Hosts aus, wobei ein violetter Diagnosebildschirm angezeigt wird. Die Standardwartezeit beträgt dann 10 Minuten.

Problemumgehung: Keine.

- **Wenn IPv6 in einem vCenter Server-System mit DPUs deaktiviert ist, können Sie keine DPUs verwalten.**

Obwohl der vSphere Client den Vorgang zulässt, können Sie die DPUs nicht verwenden, wenn Sie IPv6 auf einem ESXi-Host mit DPUs deaktivieren, da die interne Kommunikation zwischen dem Host und den Geräten von IPv6 abhängt. Das Problem betrifft nur ESXi-Hosts mit DPUs.

Problemumgehung: Stellen Sie sicher, dass IPv6 auf ESXi-Hosts mit DPUs aktiviert ist.

- **Wenn während des Herunterfahrens oder Neustarts eines ESXi-Hosts ein PCI-Passthrough zu einer DPU aktiv ist, schlägt der Host mit einem violetten Diagnosebildschirm fehl**

Wenn eine aktive virtuelle Maschine zum Zeitpunkt des Herunterfahrens oder Neustarts eines ESXi-Hosts einen PCI-Passthrough (SR-IOV or UPT) zu einer DPU aufweist, schlägt der Host mit einem violetten Diagnosebildschirm fehl. Das Problem ist spezifisch für Systeme mit DPUs und nur im Fall von VMs, die PCI-Passthrough zur DPU verwenden.

Problemumgehung: Stellen Sie vor dem Herunterfahren oder Neustart eines ESXi-Hosts sicher, dass sich der Host im Wartungsmodus befindet oder dass keine VMs ausgeführt werden, die PCI-Passthrough zu einer DPU verwenden. Wenn Sie Optionen für den automatischen Start einer virtuellen Maschine verwenden, stoppt der Autostart-Manager solche VMs vor dem Herunterfahren oder Neustart eines Hosts.

Netzwerkprobleme

- **Pensulator-DPUs unterstützen das LLDP (Link Layer Discovery Protocol) auf physischen Switch-Ports von ESXi-Hosts nicht**

Wenn Sie LLDP auf einem ESXi-Host mit einer DPU aktivieren, kann der Host keine LLDP-Pakete empfangen.

Problemumgehung: Keine.

- **Es ist nicht möglich, Mellanox ConnectX-5- und ConnectX-6-Karten mit Modell 1 Level 2 und Modell 2 für den ENS-Modus (Enhanced Network Stack) in vSphere 8.0 zu verwenden**

Aufgrund von Hardwarebeschränkungen werden Modell 1 Level 2 und Modell 2 für den ENS-Modus (Enhanced Network Stack) in vSphere 8.0 von ConnectX-5- und ConnectX-6-Adapterkarten nicht unterstützt.

Problemumgehung: Verwenden Sie Karten des Typs Mellanox ConnectX-6 Lx und ConnectX-6 Dx oder neuere Karten, die ENS Modell 1 Level 2 und Modell 2A unterstützen.

- **Wenn Sie einen ESXi-Host nach dem Aktivieren oder Deaktivieren von SR-IOV mit dem `icen`-Treiber beim Konfigurieren eines Transportknotens im ENS-Unterbrechungsmodus auf diesem Host nicht neu starten, erhalten einige virtuelle Maschinen möglicherweise keine DHCP-Adressen**

Nach dem Aktivieren oder Deaktivieren von SR-IOV mit dem `icen`-Treiber auf einem ESXi-Host und dem Konfigurieren eines Transportknotens im ENS-Unterbrechungsmodus funktionieren einige Rx-Warteschlangen (Empfangswarteschlangen) möglicherweise nicht, sofern Sie den Host nicht neu starten. Infolgedessen erhalten einige virtuelle Maschinen möglicherweise keine DHCP-Adressen.

Problemumgehung: Fügen Sie entweder direkt ein Transportknotenprofil hinzu, ohne SR-IOV zu aktivieren, oder starten Sie den ESXi-Host nach dem Aktivieren oder Deaktivieren von SR-IOV neu.

- **Die Installation oder das Upgrade von VMware NSX in einer vSphere-Umgebung mit DPUs schlägt möglicherweise mit einem Konnektivitätsfehler fehl**

Ein zeitweiliges Zeitproblem auf der ESXi-Hostseite kann dazu führen, dass die Installation oder das Upgrade von NSX in einer vSphere-Umgebung mit DPUs fehlschlägt. Die Datei `nsxapi.log` enthält Protokolle wie etwa `Failed to get SFHC response. MessageType MT_SOFTWARE_STATUS`.

Problemumgehung: Warten Sie 10 Minuten und wiederholen Sie die Installation oder das Upgrade von NSX.

- **Bei NICs, die den Treiber `ntg3` der Version 4.1.3 und höher verwenden, tritt Link Flapping auf**

Wenn zwei NICs, die den `ntg3`-Treiber der Version 4.1.3 und höher verwenden, direkt und nicht mit einem physischen Switch-Port verbunden sind, kann Link Flapping auftreten. Das Problem tritt nicht bei `ntg3`-Treibern mit Versionen vor 4.1.3 oder dem `tg3`-Treiber auf. Dieses Problem steht nicht im Zusammenhang mit dem gelegentlich auftretenden Energy Efficient Ethernet (EEE) Link Flapping bei solchen NICs. Die Lösung für das EEE-Problem besteht darin, einen `ntg3`-Treiber der Version 4.1.7 oder höher zu verwenden oder EEE an physischen Switch-Ports zu deaktivieren.

Problemumgehung: Aktualisieren Sie den `ntg3`-Treiber auf Version 4.1.8 und setzen Sie den neuen Modulparameter `noPhyStateSet` auf 1. Der Parameter `noPhyStateSet` ist standardmäßig auf 0 gesetzt und wird in den meisten Umgebungen nicht benötigt, es sei denn, sie sind von dem Problem betroffen.

- **Sie können die maximale Übertragungseinheit (MTU) auf einem VMware vSphere Distributed Switch nicht auf einen Wert größer als 9174 auf einer Pensando DPU einstellen**

Wenn Sie die vSphere Distributed Services Engine-Funktion mit einer Pensando DPU auf Ihrem ESXi 8.0-System aktiviert haben, können Sie die maximale Übertragungseinheit (MTU) auf einem vSphere Distributed Switch nicht auf einen Wert größer als 9174 festlegen.

Problemumgehung: Keine.

Speicherprobleme

- **Aufgrund eines im Content Based Read Cache (CBRC) auftretenden Fehlers im Zusammenhang mit einem Digest-Vorgang können keine Snapshots von virtuellen Maschinen erstellt werden**

Eine seltene Racebedingung bei der Zuweisung einer Inhalts-ID während der Aktualisierung der CBRC-Digest-Datei kann zu einer Diskrepanz zwischen der Inhalts-ID auf der Datenfestplatte und der Digest-Festplatte führen. Infolgedessen können Sie keine VM-Snapshots erstellen. Im Backtrace wird eine Fehlermeldung ähnlich der folgenden angezeigt: `An error occurred while saving the snapshot: A digest operation has failed.` Die Aufgabe zum Erstellen des Snapshots wird bei einem erneuten Versuch abgeschlossen.

Problemumgehung: Wiederholen Sie die Snapshot-Erstellung.

- **vSphere Storage vMotion-Vorgänge könnten in einer vSAN-Umgebung aufgrund einer nicht authentifizierten Sitzung des NFC-Managers (Network File Copy) fehlschlagen**

Migrationen in einen vSAN-Datenspeicher mithilfe von vSphere Storage vMotion von virtuellen Maschinen mit mindestens einem Snapshot und mehreren virtuellen Festplatten mit unterschiedlicher Speicherrichtlinie könnten fehlschlagen. Das Problem tritt aufgrund einer nicht authentifizierten Sitzung des NFC-Managers auf, da der Simple Object Access Protocol (SOAP)-Body die zulässige Größe überschreitet.

Problemumgehung: Migrieren Sie zuerst den VM-Start-Namespace und nur eine der virtuellen Festplatten. Führen Sie nach Abschluss des Vorgangs nur eine Festplattenmigration der verbleibenden beiden Festplatten durch.

- **Die VASA API-Version wird nach dem Upgrade auf vCenter Server 8.0 nicht automatisch aktualisiert**

vCenter Server 8.0 unterstützt die VASA API-Version 4.0. Nach dem Upgrade Ihres vCenter Server-Systems auf Version 8.0 ändert sich die VASA API-Version jedoch möglicherweise nicht automatisch auf 4.0. Dieses Problem tritt in den folgenden beiden Fällen auf:

- a Wenn ein VASA-Anbieter, der die VASA API-Version 4.0 unterstützt, bei einer früheren Version von VMware vCenter registriert ist, bleibt die VASA API-Version nach dem Upgrade auf VMware vCenter 8.0 unverändert. Wenn Sie beispielsweise ein VMware vCenter-System der Version 7.x mit einem registrierten VASA-Anbieter aktualisieren, der sowohl die VASA API-Versionen 3.5 als auch 4.0 unterstützt, ändert sich die VASA API-Version nicht automatisch auf 4.0, obwohl der VASA-Anbieter die VASA API-Version 4.0 unterstützt. Wenn Sie nach dem Upgrade zu **vCenter Server > Konfigurieren > Speicheranbieter** navigieren und die Registerkarte **Allgemein** des registrierten VASA-Anbieters erweitern, wird weiterhin die VASA API-Version 3.5 angezeigt.
- b Wenn Sie einen VASA-Anbieter, der die VASA API-Version 3.5 unterstützt, mit einem VMware vCenter 8.0-System registrieren und die VASA API-Version auf 4.0 aktualisieren, wird auch nach dem Upgrade weiterhin die VASA API-Version 3.5 angezeigt.

Problemumgehung: Heben Sie die Registrierung des VASA-Anbieters auf dem VMware vCenter 8.0-System auf und registrieren Sie ihn erneut.

Probleme bei vCenter Server und dem vSphere Client

- **Wenn Sie ein benutzerdefiniertes Update-Repository mit nicht vertrauenswürdigen Zertifikaten verwenden, schlägt das vCenter Server-Upgrade oder das Update mithilfe von vCenter Lifecycle Manager-Workflows auf vSphere 8.0 möglicherweise fehl**

Wenn Sie ein benutzerdefiniertes Update-Repository mit selbstsignierten Zertifikaten verwenden, denen die VMware Certificate Authority (VMCA) nicht vertraut, kann vCenter Lifecycle Manager keine Dateien aus einem solchen Repository herunterladen. Dies führt dazu, dass vCenter Server-Upgrade- oder Aktualisierungsvorgänge mithilfe von vCenter Lifecycle Manager-Workflows mit dem Fehler `Failed to load the repository manifest data for the configured upgrade` fehlschlagen.

Problemumgehung: Verwenden Sie zur Durchführung des Upgrades die CLI, das GUI-Installationsprogramm oder die Virtual Appliance Management Interface (VAMI). Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [90259](#).

- **ESXi-Hosts reagieren möglicherweise nicht mehr, und es wird eine vpxa-Dump-Datei angezeigt, weil in seltenen Fällen die Dateideskriptoren für die Anforderungswarteschlange auf vpxa nicht ausreichen**

In seltenen Fällen kann es bei lange dauernden Anforderungen an den vpxa-Dienst, etwa beim Warten auf Zugang zu einem langsamen Datenspeicher, in der Anforderungswarteschlange auf vpxa zu einer Überschreitung des Limits der Dateideskriptoren kommen. Infolgedessen reagieren ESXi-Hosts dann unter Umständen kurzzeitig nicht mehr, und eine Datei `vpxa-zdump.00*` wird im Verzeichnis `/var/core` angezeigt. Die vpxa-Protokolle enthalten die Zeile `Too many open files`.

Probleumlösung: Keine. Der vpxa-Dienst wird automatisch neu gestartet, um das Problem zu beheben.

- **Zu CNS-Blockvolumes (Cloud Native Storage), die per API in einer heterogenen vCenter-Umgebung erstellt wurden, wird eine Fehlermeldung angezeigt**

Wenn in Ihrer Umgebung vCenter Server-Systeme der Version 8.0 und 7.x vorhanden sind, können CNS-Blockvolumes (Cloud Native Storage) per API erstellt werden, allerdings wird im vSphere Client möglicherweise eine Fehlermeldung angezeigt, wenn Sie Detailangaben zum CNS-Volumen abrufen. Es wird dann eine Fehlermeldung ähnlich der folgenden angezeigt: `Failed to extract the requested data. Check vSphere Client logs for details. + TypeError: Cannot read properties of null (reading 'cluster')`. Das Problem tritt nur auf, wenn Sie Volumes überprüfen, die von vCenter Server Version 7.x unter Verwendung des vSphere Client von vCenter Server Version 8.0 verwaltet werden.

Probleumlösung: Melden Sie sich beim vSphere Client eines vCenter Server-Systems der Version 7.x an, um die Volume-Eigenschaften zu überprüfen.

- **Im vSphere Client werden keine Banner-Benachrichtigungen für Importe von Verlaufsdaten angezeigt**

Aufgrund eines Back-End-Problems werden im vSphere Client keine Banner-Benachrichtigungen zur Hintergrundmigration von Verlaufsdaten angezeigt.

Probleumlösung: Verwenden Sie die vCenter Server-Verwaltungsschnittstelle als Alternative zum vSphere Client. Weitere Informationen finden Sie unter [Überwachen und Verwalten der Migration von Verlaufsdaten](#).

- **Wenn Sie die virtuelle vSphere-Infrastruktur zu mehr als 90 % auslasten, werden die ESXi-Hosts möglicherweise zeitweise vom vCenter Server getrennt**

In seltenen Fällen, wenn die virtuelle vSphere-Infrastruktur kontinuierlich mehr als 90 % ihrer Hardwarekapazität nutzt, kann es vorkommen, dass einige ESXi-Hosts zeitweise die Verbindung zum vCenter Server unterbrechen. Die Verbindung wird in der Regel innerhalb weniger Sekunden wiederhergestellt.

Probleumlösung: Wenn die Verbindung zu vCenter Server versehentlich nicht innerhalb weniger Sekunden wiederhergestellt wird, verbinden Sie die ESXi-Hosts mithilfe des vSphere Client manuell neu.

- **Die Auslastungsansicht von Ressourcenpools und Clustern wird möglicherweise nicht automatisch aktualisiert, wenn Sie das Objekt ändern**

Wenn Sie die Ansicht **Auslastung** auf der Registerkarte **Überwachen** für einen Ressourcenpool oder einen Cluster bereits geöffnet haben und dann den Ressourcenpool oder Cluster ändern, wird die Ansicht möglicherweise nicht automatisch aktualisiert. Wenn Sie beispielsweise die Ansicht **Auslastung** eines Clusters öffnen und dann einen anderen Cluster auswählen, werden unter Umständen weiterhin die Statistiken des ersten Clusters angezeigt.

Probleumlösung: Klicken Sie auf das Aktualisierungssymbol.

VM-Verwaltungsprobleme

- **Beim Hinzufügen einer vorhandenen virtuellen Festplatte zu einer neuen virtuellen Maschine wird unter Umständen eine Fehlermeldung angezeigt, dass die VM-Konfiguration abgelehnt wird**

Wenn Sie unter Verwendung des VMware Host Client einer neuen virtuellen Maschine eine vorhandene virtuelle Festplatte hinzufügen, scheitert der Vorgang eventuell mit einer Fehlermeldung ähnlich der folgenden: `The VM configuration was rejected. Please see browser Console`. Das Problem tritt auf, weil der VMware Host Client eventuell einige Eigenschaften, beispielsweise zum Festplattencontroller, nicht abrufen kann.

Problemumgehung: Klicken Sie nach dem Auswählen einer Festplatte und Aufrufen der Seite **Bereit zum Abschließen** nicht auf die Schaltfläche **Beenden**. Wechseln Sie stattdessen zum vorherigen Schritt, warten Sie ab, bis die Seite geladen ist, und klicken Sie dann auf **Weiter > Beenden**.

Probleme bei Sicherheitsfunktionen

- **Bei Verwendung einer RSA-Schlüsselgröße kleiner als 2048 Bit scheitert die RSA-Signaturerstellung**

Ab vSphere 8.0 verwendet ESXi den FIPS-Anbieter OpenSSL 3.0. Entsprechend der FIPS 186-4-Anforderung muss die RSA-Schlüsselgröße für jede Signaturerstellung mindestens 2048 Bit betragen, und die Signaturerstellung mit SHA1 wird nicht unterstützt.

Problemumgehung: Verwenden Sie eine RSA-Schlüsselgröße größer als 2048.

Probleme bei vSphere Lifecycle Manager

- **Wenn Sie einen ESXi-Host verwenden, der aus einem Hostprofil mit aktivierter statusbehafteter Installation als Image bereitgestellt wurde, um andere ESXi-Hosts in einem Cluster bereitzustellen, schlägt der Vorgang fehl**

Wenn Sie ein Image eines ESXi-Hosts, das von einem Hostprofil mit aktivierter statusbehafteter Installation bereitgestellt wurde, extrahieren, um andere ESXi-Hosts in einem vSphere Lifecycle Manager-Cluster bereitzustellen, schlägt der Vorgang fehl. Im vSphere Client wird ein Fehler ähnlich dem folgenden angezeigt: `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.`

Problemumgehung: Verwenden Sie einen anderen Host aus dem Cluster, um ein Image zu extrahieren.

- **Wenn eine parallele Standardisierungsaufgabe fehlschlägt, wird nicht die richtige Anzahl an ESXi-Hosts angezeigt, die den Vorgang übergeben oder übersprungen haben**

Mit vSphere 8.0 können Sie vSphere Lifecycle Manager aktivieren, um alle Hosts, die sich im Wartungsmodus befinden, parallel statt nacheinander zu standardisieren. Wenn jedoch eine parallele Standardisierungsaufgabe fehlschlägt, sehen Sie im vSphere Client möglicherweise nicht die richtige Anzahl an Hosts, die den Vorgang bestanden, nicht bestanden oder übersprungen haben, oder sehen überhaupt keine solche Anzahl. Das Problem wirkt sich nicht auf die vSphere Lifecycle Manager-Funktionalität aus, sondern nur auf die Berichterstellung im vSphere Client.

Problemumgehung: Keine.

- **Beim Versuch, vSphere Lifecycle Manager-Images auf ESXi-Hosts mit einer früheren Version als 8.0 bereitzustellen, werden Fehlermeldungen angezeigt**

Ab ESXi 8.0 gibt es die Option, gewünschte Status-Images explizit bereitzustellen. Dabei werden Depotkomponenten aus dem vSphere Lifecycle Manager-Depot auf die ESXi-Hosts heruntergeladen, ohne die Software- und Firmware-Updates unmittelbar anzuwenden. Das Staging von Images wird jedoch nur auf einem ESXi-Host der Version 8.0 oder höher unterstützt. Der Versuch, ein vSphere Lifecycle Manager-Image auf ESXi-Hosts einer früheren Version als 8.0 bereitzustellen, führt zu Meldungen, die besagen, dass das Staging solcher Fehler fehlgeschlagen ist und die Hosts übersprungen wird. Dies entspricht dem erwarteten Verhalten und ist kein Anzeichen für eine Fehlfunktion, da alle ESXi-Hosts der Version 8.0 oder höher mit dem angegebenen gewünschten Image bereitgestellt werden.

Problemumgehung: Keine. Nachdem Sie sich vergewissert haben, dass die betroffenen ESXi-Hosts eine frühere Version als 8.0 aufweisen, können Sie die Fehler ignorieren.

- **Bei einer Wartungsaufgabe unter Verwendung von vSphere Lifecycle Manager tritt bei ESXi-Hosts mit DPUs eventuell gelegentlich ein Fehler auf**

Wenn Sie auf ESXi-Hosts mit DPUs eine Wartung von vSphere Lifecycle Manager starten, erfolgt beim Host wie erwartet ein Upgrade und Neustart. Nach dem Neustart und vor Abschluss der Wartungsaufgabe wird allerdings unter Umständen eine Fehlermeldung ähnlich der folgenden angezeigt:

```
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.
```

Dies ist ein selten auftretendes Problem, das verursacht wird durch eine gelegentlich auftretende Zeitüberschreitung bei der auf die Wartung folgenden Prüfung der DPU.

Problemumgehung: Starten Sie den ESXi-Host neu und führen Sie die Konformitätsprüfung bei vSphere Lifecycle Manager erneut durch, zu der auch die auf die Wartung folgende Prüfung gehört.

Probleme mit VMware Host Client

- **VMware Host Client zeigt möglicherweise falsche Beschreibungen für Schweregrad-Ereigniszustände an**

Wenn Sie im VMware Host Client nach den Beschreibungen der Schweregrad-Ereigniszustände eines ESXi-Hosts suchen, können sie sich von den Beschreibungen unterscheiden, die bei Verwendung von Intelligent Platform Management Interface (IPMI) oder Lenovo XClarity Controller (XCC) angezeigt werden. Beispielsweise kann im VMware Host Client die Beschreibung des Schweregrad-Ereigniszustands für die PSU-Sensoren `Transition to Non-critical from OK` lauten, während sie im XCC und IPMI `Transition to OK` lautet.

Problemumgehung: Überprüfen Sie die Beschreibungen für Schweregrad-Ereigniszustände mithilfe des ESXCLI-Befehls `esxcli hardware ipmi sdr list` und Lenovo XCC.

Probleme mit dem Gastbetriebssystem

- **Das Linux-Gastbetriebssystem kann den Startvorgang nicht abschließen, wenn die Neuordnung von Direct Memory Access (DMA) aktiviert ist**

Wenn die erweiterte Prozesseinstellung `Enable IOMMU in this virtual machine` auf einer virtuellen Maschine aktiviert ist und das Gastbetriebssystem die DMA-Neuordnung aktiviert hat, kann das Linux-Gastbetriebssystem den Startvorgang möglicherweise nicht abschließen. Dieses Problem betrifft VMs mit Hardwareversion 20 und einer Linux-Distribution, die bestimmte Patches enthält, die im Linux-Kernel 5.18 für eine VMCI-Funktion eingeführt wurden, einschließlich, aber nicht beschränkt auf aktuelle Versionen von RHEL 8.7, Ubuntu 22.04 und 22.10 und SLES15 SP3 und SP4.

Problemumgehung: Setzen Sie die erweiterte Option `vmci.dmaDatagramSupport` auf `FALSE` oder deaktivieren Sie die Option `Enable IOMMU in this virtual machine`. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [89683](#).

- **Das Gastbetriebssystem einer VM reagiert möglicherweise aufgrund eines Kommunikationsausfalls über die VMCI (Virtual Machine Communication Interface) nicht mehr**

Unter sehr spezifischen Umständen kann es bei der Ausführung eines vSphere vMotion-Vorgangs auf einer virtuellen Maschine parallel zu einem Vorgang, der VMCI-Datagramme sendet, bei Diensten, die VMCI-Datagramme verwenden, zu einer unerwarteten Kommunikation oder einem Kommunikationsverlust kommen. Unter denselben Bedingungen kann das Problem auch beim Wiederherstellen eines Arbeitsspeicher-Snapshots, beim Fortsetzen einer angehaltenen VM oder beim Hinzufügen von CPUs im laufenden Betrieb auftreten. Dies führt dazu, dass das Gastbetriebssystem, das von Diensten abhängt, die über VMCI kommunizieren, möglicherweise nicht mehr reagiert. Das Problem kann sich auch auf Dienste auswirken, die vSockets über VMCI verwenden. Dieses Problem hat keine Auswirkungen auf VMware Tools. Das Problem ist spezifisch für VMs auf Hardwareversion 20 mit einer Linux-Distribution, die bestimmte Patches enthält, die im Linux-Kernel 5.18 für eine VMCI-Funktion eingeführt wurden, einschließlich, aber nicht beschränkt auf aktuelle Versionen von RHEL 8.7, Ubuntu 22.04 und 22.10 und SLES15 SP3 und SP4.

Problemumgehung: Setzen Sie die erweiterte Option `vmci.dmaDatagramSupport` auf `FALSE`.
Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel [89683](#).