

VMware vCenter 6.5 Update 3 Release Notes

vCenter Server 6.5 Update 3 | JUL 2 2019 | ISO Build 14020092
vCenter Server Appliance 6.5 Update 3 | JUL 2 2019 | ISO Build 14020092

Check for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

- [What's New](#)
- [Earlier Releases of vCenter Server 6.5](#)
- [Patches Contained in this Release](#)
- [Upgrade Notes for This Release](#)
- [Resolved Issues](#)
- [Known Issues](#)

What's New

The vCenter Server 6.5 Update 3 release includes the following list of new features.

- With vCenter Server 6.5 Update 3, events related to adding, removing, or modifying user roles display the user that initiates the changes.
- **vSphere Auditing Improvements:** vCenter Server 6.5 Update 3 improves VMware vCenter Single Sign-On auditing by adding events for the following operations: user management, login, group creation, identity source, and policy updates. The new feature is available only for vCenter Server Appliance with an embedded Platform Services Controller and not for vCenter Server for Windows or vCenter Server Appliance with an external Platform Services Controller. Supported identity sources are vsphere.local, Integrated Windows Authentication (IWA), and Active Directory over LDAP.
- **External database support:** vCenter Server 6.5 Update 3 adds support to Microsoft SQL Server 2014 SP3.
- For Photon OS updates, see [VMware vCenter Server Appliance Photon OS Security Patches](#).

Earlier Releases of vCenter Server 6.5

Features and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 6.5 are:

- [VMware vCenter Server 6.5 Update 2g Release Notes](#)
- [VMware vCenter Server 6.5 Update 2d Release Notes](#)
- [VMware vCenter Server 6.5 Update 2c Release Notes](#)
- [VMware vCenter Server 6.5 Update 2b Release Notes](#)
- [VMware vCenter Server 6.5 Update 2 Release Notes](#)
- [VMware vCenter Server 6.5 Update 1g Release Notes](#)
- [VMware vCenter Server 6.5 Update 1e Release Notes](#)
- [VMware vCenter Server 6.5 Update 1d Release Notes](#)
- [VMware vCenter Server 6.5 Update 1c Release Notes](#)
- [VMware vCenter Server 6.5 Update 1b Release Notes](#)
- [VMware vCenter Server 6.5 Update 1 Release Notes](#)
- [VMware vCenter Server 6.5.0d Release Notes](#)
- [VMware vCenter Server 6.5.0c Release Notes](#)
- [VMware vCenter Server 6.5.0b Release Notes](#)
- [VMware vCenter Server 6.5.0a Release Notes](#)
- [VMware vSphere 6.5 Release Notes](#)

For internationalization, compatibility, installation and upgrades, product support notices, and features see the [VMware vSphere 6.5 Release Notes](#).

Patches Contained in This Release

This release of vCenter Server 6.5 Update 3 delivers the following patches. See the [VMware Patch Download Center](#) for more information on downloading patches.

- [Security Patch for VMware vCenter Server 6.5 Update 3](#)
- [Full Patch for VMware vCenter Server Appliance 6.5 Update 3](#)

Security Patch for VMware vCenter Server 6.5 Update 3

Third Party Product fixes (for example: JRE, tcServer). This patch is applicable for vCenter Server for Windows, Platform Services Controller for Windows, and vSphere Update Manager.

NOTE: This patch updates only the JRE version 1.8.0_212.

For vCenter Server and Platform Services Controller for Windows

Download Filename	VMware-VIMPatch-T-6.5.0-14020092.iso
Build	14020092
Download Size	40.9 MB
md5sum	7daaa2df025373d6eb54456b27cb9fcd
sha1checksum	cc934b7a35e171713285758a50f5e86d6a092d3b

These vCenter Server components depend on JRE and have to be patched:

- vCenter Server
- Platform Services Controller
- vSphere Update Manager

Download and Installation

You can download this patch by going to the [VMware Patch Download Center](#) and choosing **VC** from the **Select a Product** drop-down menu.

1. Mount the [VMware-VIMPatch-T-6.5.0-14020092.iso](#) to the system where the vCenter Server component is installed.
2. Double-click [ISO_mount_directory/autorun.exe](#).
3. In the vCenter Server Java Components Update wizard, click **Patch All**.

Full Patch for VMware vCenter Server Appliance 6.5 Update 3

Product Patch for vCenter Server Appliance 6.5 containing VMware software fixes, security fixes, and Third Party Product fixes (for example: JRE and tcServer).

This patch is applicable to the vCenter Server Appliance and Platform Services Controller Appliance.

For vCenter Server and Platform Services Controller Appliances

Download Filename	VMware-vCenter-Server-Appliance-6.5.0.30000-14020092-patch-FP.iso
Build	14020092
Download Size	1710.6 MB
md5sum	cab35495c606846d5b959499bc18a2a9
sha1checksum	ee6660ffca04065412414f4aab9be1d68510bad

Download and Installation

You can download this patch by going to the [VMware Patch Download Center](#) and choosing **VC** from the **Select a Product** drop-down menu.

1. Attach the [VMware-vCenter-Server-Appliance-6.5.0.30000-14020092-patch-FP.iso](#) file to the vCenter Server Appliance CD or DVD drive.
2. Log in to the appliance shell as root and run the commands given below:
 - To stage the ISO:


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


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


```
software-packages install --staged
```

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

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

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

For issues resolved in this patch see [Resolved Issues](#).

For Photon OS updates, see [VMware vCenter Server Appliance Photon OS Security Patches](#).

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

Upgrade Notes for This Release

Important: Upgrades and migrations from vCenter Server 6.5 Update 3 to vCenter Server 6.7 Update 3 and above are supported. For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article [67077](#).

Upgrades or migration of vCenter Server earlier than 5.5 Update 3b when the environment is with an external vCenter Single Sign-On to vCenter Server 6.5 Update 3 with an external Platform Services Controller are unsupported. For example, to upgrade or migrate vCenter Server 5.5 with an external vCenter Single Sign-On to vCenter Server 6.5 Update 3 with an external Platform Services Controller, you must first update to vCenter Server 5.5 Update 3b and then perform the upgrade or migration to vCenter Server 6.5 Update 3.

vCenter Server 5.5 Update 3b build numbers are:

- vCenter Server 5.5 Update 3b, build 3252642

- vCenter Server Appliance 5.5 Update 3b, build 3255668

Upgrades or migration of vCenter Server 5.5 and later with an embedded vCenter Single Sign-On to vCenter Server 6.5 Update 3 with an embedded Platform Services Controller are supported scenarios.

Resolved Issues

The resolved issues are grouped as follows.

- [Miscellaneous Issues](#)
- [Guest OS Issues](#)
- [Installation, Upgrade, Convergence, and Migration Issues](#)
- [VMware High Availability and Fault Tolerance Issues](#)
- [Security Issues](#)
- [vMotion Issues](#)
- [Virtual Machine Management Issues](#)
- [CIM and API Issues](#)
- [Networking Issues](#)
- [Server Configuration Issues](#)
- [Storage Issues](#)
- [Backup and Restore Issues](#)
- [Licensing Issues](#)
- [vCenter Server, vSphere Web Client, and vSphere Client Issues](#)
- [vSAN Issues](#)
- [Tools Issues](#)

Miscellaneous Issues

- **An ESXi host might get disconnected from the vCenter Server system**

The vpxa service might fail due to excessive memory usage when iterating on a large directory tree. As a result, an ESXi host might get disconnected from the vCenter Server system.

This issue is resolved in this release.

- **Stored procedures for the cleanup of tasks and events in the vCenter Server Appliance might fail**

Stored procedures for the cleanup of tasks and events in the vCenter Server Appliance might fail with an error `ERROR FOREACH expression must not be null` in the `postgresql-XX.logs`.

This issue is resolved in this release.

- **A vCenter Server system might cancel the RPC calls due to a race in the communication between vCenter Server and the ESXi hosts**

A vCenter Server system might cancel the RPC calls due to a race in the VM Object Management Infrastructure RPC ping logic. As a result, you might observe operation failures.

This issue is resolved in this release.

- **When you try to power on a virtual machine with a full CPU reservation or perform a migration by using vSphere vMotion, the operation might fail**

If the ESXi hosts in a cluster have CPU size differences, the power-on operation or migration by using vSphere vMotion of a virtual machine that has a full CPU reservation might fail. Operations involving virtual machines with full CPU reservations might result in constraint check failures because of the CPU size differences.

This issue is resolved in this release. The fix relaxes the constraint check.

- **In an environment with a heavy workload, the VMware Security Token Service (vmware-stds) might stop responding and cause login failures**

The vmware-stds service has a fixed amount of allocated memory in the `setenv.sh` file but the memory size might be insufficient in an environment with a heavy workload. As a result, the vmware-stds service might stop responding and cause login failures.

This issue is resolved in this release. The fix dynamically sets the memory allocation for the vmware-stds service at the start time, based on the size of the deployment.

- **A scheduled task to take snapshots of multiple virtual machines might start immediately instead of at the scheduled time**

When you schedule a task to take snapshots of multiple virtual machines, the task starts immediately instead of at the scheduled time.

This issue is resolved in this release.

- **You might be unable to start the vCenter Server services due to an invalid JSON file**

The vCenter Server services stat file might become corrupt due to disk I/O issues or a disk full error. When you try to restart the vCenter Server services, the file is empty and therefore detected as an invalid JSON file. As a result, the vCenter Server services fail to start.

This issue is resolved in this release.

- **When you enable vSphere Storage Distributed Resource Scheduler (vSphere Storage DRS) and anti-affinity rules, the vpxd service might stop responding**

When the vpxd service checks for violation of the DRS affinity rule for a virtual machine, the vpxd service might stop responding due to invalid memory access.

This issue is resolved in this release.

Guest OS Issues

- **You cannot set a primary virtual NIC**

You cannot customize the vCenter Server Appliance guest OS to set a virtual NIC as a primary NIC.

This issue is resolved in this release. With this fix, you can customize a virtual NIC and set it up as a primary NIC if it is the first NIC, has a static IPv4 address, and a configured gateway.

Installation, Upgrade, Convergence, and Migration Issues

- **The vCenter Server Convergence Tool might fail to convert an external Platform Services Controller to an embedded Platform Services Controller due to a command failure**

When you upgrade from vCenter Server 6.5 to 6.5 Update 2d, the `vmafd_cli` command cannot return the LDU entries and fails with a `Converge Failed to get ldu id of localhost` error. As a result, the vCenter Server Convergence Tool might fail to convert an external Platform Services Controller to an embedded Platform Services Controller.

This issue is resolved in this release.

- **After the convergence of a vCenter Server Appliance with an external Platform Services Controller, the IPv6 loopback address might be replaced by an IPv4 loopback address**

If you convert instances of vCenter Server Appliance with an external Platform Services Controller to vCenter Server Appliance with an embedded Platform Services Controller connected in Embedded Linked Mode, the loopback address `::1` in pure IPv6 setup might be removed from the `/etc/resolv.conf` file. An IPv4 loopback address, such as `[127.0.0.1]`, might be added.

This issue is resolved in this release.

- **Certifications might be lost after a convergence of a vCenter Server instance with an external Platform Services Controller to a vCenter Server instance with an embedded Platform Services Controller**

Key Management Server (KMS) and Certificate Authority (CA) certificates might be lost after a convergence of the vCenter Server instance with an external Platform Services Controller to a vCenter Server instance with an embedded Platform Services Controller. You might see a warning similar to:

`Not connected (Trust not established. View Details)`

This issue is resolved in this release.

VMware High Availability and Fault Tolerance Issues

- **The Fault Domain Manager (FDM) might become unavailable when you migrate a virtual machine by using vSphere vMotion**

When the process of migration of a virtual machine by using vSphere vMotion finishes, the virtual machine might not remain in the inventory. As a result, the FDM might become unavailable when trying to access the virtual machine.

This issue is resolved in this release.

- **Configuration of VMware vCenter Server High Availability might fail with an error that the PNID host name does not match the IP address**

Configuration of vCenter Server High Availability might fail with an error that the PNID host name does not match the IP address.

This issue is resolved in this release.

Security Issues

- **Update to the Spring Framework**

The Spring Framework is updated to version 4.3.22.

- **Upgrade of Eclipse Jetty**

Eclipse Jetty is upgraded to version 9.4.14.v20181114.

- **Update to PostgreSQL**

PostgreSQL is updated to version 9.6.13.

- **Update to cURL**

cURL in the vCenter Server Appliance is updated to version 7.64.

- **Update of the JSON processor package**

The JSON processor package is updated to version 2.9.8.

- **Numbering of firewall rules might unexpectedly change if you reorder the rules**

If you create more than 9 firewall rules in a vCenter Server Appliance and change the order, setting a rule with a double-digit numbering among rules with one-digit numbering, the numbering might change. For instance, if you move a rule with number 10, such as `10 RETURN all -- X.X.X.10 anywhere`, to position 2, the numbering might change to `2 RETURN all -- X.X.X.10 anywhere`.

This issue is resolved in this release.

- **Users with a Virtual Machine user role might not be able to edit the scheduled tasks that they created**

Users with permissions on a folder level, such as Virtual Machine user, might not be able to run, edit, or delete the scheduled tasks that they create.

This issue is resolved in this release.

- **Update to Apache Struts**

Apache Struts is updated to version 2.5.20.

- **Update to the OpenSSH**

The OpenSSH version is updated to version 7.4p1-8.

- **Update to the Network Time Protocol (NTP) daemon**

The NTP daemon is updated to version 4.2.8p12-3.

- **Security vulnerabilities with jQuery version 2.1.4**

The jQuery version 2.1.4 might have security vulnerabilities while performing AJAX calls to Domino agents.

This issue is resolved in this release. This fix upgrades jQuery and the jQuery UI to version 3.3.1.

- **Update to OpenSSL**

The OpenSSL package is updated to version openssl-1.0.2r.

- **Update to the Apache HTTP Server**

The Apache HTTP Server (httpd) is updated to version 2.4.39 to resolve security issues with identifiers CVE-2019-0211, CVE-2019-2017, and CVE-2019-0215.

- **Update to JRE**

Oracle (Sun) JRE is updated to version 1.8.212.

- **Update to the Python library**

The Python third-party library is updated to version 2.7.16/3.5.6.

- **Update to the Apache Commons BeanUtils package**

The Apache Commons BeanUtils package is updated to version 1.9.3.

- **Update to the Apache Tomcat server**

The Apache Tomcat server is updated to version 8.5.40.

- **After the Active Directory server is temporarily inaccessible, the user and group permissions for the Active Directory domain are removed**

vCenter Server regularly validates users and groups against the Windows Active Directory domain. If an identity is removed, the vCenter Server system removes the permissions associated with it. If the Active Directory server is unreachable during the validation process, the vCenter Server system might incorrectly interpret this as removal of all domain users and groups and might remove the permissions associated with them.

This issue is resolved in this release. The fix differentiates between a missing identity and no connection.

- **Update to Photon OS kernel**

Photon OS kernel is updated to version 4.4.182 to resolve security issues with identifiers CVE-2019-11477, CVE-2019-11478, and CVE-2019-11479.

vMotion Issues

- **An ESXi host might be displayed as not responding**

An ESXi host might be marked as not responding and unmanageable by vCenter Server. As part of the load balancing process, vSphere DRS might trigger multiple attempts to migrate the same virtual machine by using vSphere vMotion. If the ESXi host loses connectivity to vCenter Server before the migration of the virtual machine completes, even if the connectivity is recovered for the subsequent migrations of the same virtual machine, the vpxa agent fails to send heartbeat to the vpxd service. As a result, the vpxd service marks the ESXi host as unresponsive.

This issue is resolved in this release.

- **Expanding the disk of a virtual machine by using VMware vRealize Automation might fail with an error for insufficient disk space on a datastore**

If vSphere Storage DRS does not provide a recommendation while you run an operation to expand the disk of a virtual machine by using VMware vRealize Automation, the operation might fail, because the current datastore might not have enough space. This happens when Storage DRS picks a wrong matching disk for the operation. As a result, you might see the error **Insufficient disk space on datastore**.

This issue is resolved in this release.

- **You cannot perform a migration by using vSphere vMotion when the virtual machine is configured with a local datastore swap**

If a virtual machine is configured to use a local datastore swap and you select the **Change compute resource only** migration type, the virtual machine cannot find any compatible resource. As a result, you cannot perform a migration by using vSphere vMotion.

This issue is resolved in this release.

Virtual Machine Management Issues

- **Windows virtual machines might fail when the OS is reset**

Windows virtual machines might fail when the OS is reset. The reset might be a result of internal issues, but the issue might also occur upon a normal manual reset.

This issue is resolved in this release.

- **You might not see other hard disks information in the VM Hardware panel of the vSphere Web Client**

In the vSphere Web Client, when you click the **Summary** tab for a selected virtual machine, you might see no other hard disks information in the **VM Hardware** panel.

This issue is resolved in this release.

- **Orphaned snapshot entries in the VPX_TEXT_ARRAY table might increase the size of the vCenter Server database**

When you create a snapshot of a virtual machine, multiple entries might be added to the **VPX_TEXT_ARRAY** table of the vCenter Server database. Deleting the snapshot might fail to remove these entries causing the increase of the database size. As a result, the vCenter Server system might slow down and stop responding.

This issue is resolved in this release.

- **A clone operation that involves addition of multiple disks might intermittently fail with an InvalidDatastorePath error**

Operations for cloning virtual machines that involve adding multiple disks might intermittently fail with the following error: **VmprovWorkflow: vim.fault.InvalidDatastorePath.**

This issue is resolved in this release.

- **Metrics from dynamic counters, including guest virtual machine counters, are not populated**

Metrics from guest virtual machine counters become available on an ESXi host dynamically when you power on the virtual machine. The vpxa service reports changes in the ESXi host to the vCenter Server system. However, the vpxa service cannot report availability of new counters on the ESXi host to the vCenter Server system. As a result, the Performance Manager APIs of the vCenter Server system cannot query the new counters.

This issue is resolved in this release. The fix creates a new hostd poller in the vpxa service that queries hostd once in every 5 minutes for any new counters that are added dynamically on hostd. The host-sync process reports any new counters to the vpxa service.

CIM and API Issues

- **API queries might time out when there are many objects associated with tags**

API calls, such as **listAttachedObjects**, **listAttachedObjectsOnTags**, and **listAllAttachedObjectsOnTags** might take very long to complete and ultimately time out, when many objects are associated with each tag.

This issue is resolved in this release. With this fix, the tagging APIs make batched **AuthZ** calls to vmware-vpxd to perform permission checks on all the associated objects.

- **Alarms are triggered even after using the option Reset to Green**

Alarms might be triggered even after using the option **Reset to Green** in either the vSphere Web Client or vSphere Client.

This issue is resolved in this release. With this fix, events are sent for only those sensor groups that change state within the 90-second update cycle. vCenter Server 6.5 Update 3 also adds an advanced option for configuring the synchronization interval.

- **If you remove an ESXi host that is part of a cluster from the vCenter Server system by using a com.vmware.vcenter.Host.delete REST API, both the host and the parent cluster are removed**

The **com.vmware.vcenter.Host.delete** REST API removes a standalone ESXi host from the vCenter Server system. However, if an ESXi host is part of a cluster, and you remove the ESXi host from the vCenter Server system by using the **com.vmware.vcenter.Host.delete** REST API, the parent cluster is also removed from the vCenter Server system.

This issue is resolved in this release. If you try to remove an ESXi host that is part of a cluster by using the **com.vmware.vcenter.Host.delete** REST API, an error such as **ResourceInUse** occurs.

Networking Issues

- **After an API call to an ESXi host, if a transaction element is not removed, the vpxd service might run out of memory**

In some cases, after an API call to an ESXi host, if a transaction element is not removed, the vpxd service might run out of memory. This issue occurs in large deployments with complex traffic filters configured on distributed virtual port groups.

This issue is resolved in this release.

- **vSphere Distributed Switch might become out of sync for some ESXi hosts after the upgrade to vSphere Distributed Switch 6.6**

When you migrate a virtual machine that uses a vSAN datastore from an ESXi host in one data center to an ESXi host in another data center, the port on the source distributed switch might not be released in the vCenter Server system. As a result, the vSphere Distributed Switch might become out of sync when you upgrade to vSphere Distributed Switch 6.6.

This issue is resolved in this release.

- **You cannot migrate virtual machines by using vSphere vMotion between ESXi hosts with NSX managed virtual distributed switches (N-VDS) and vSphere Standard Switches**

With vCenter Server 6.5 Update 3, you can migrate virtual machines by using vSphere vMotion between ESXi hosts with N-VDS and vSphere Standard Switches. To enable the feature, you must upgrade your vSphere system to vCenter Server 6.5 Update 3 and ESXi 6.5 Update 3 on both source and destination sites.

This issue is resolved in this release.

- **After you revert to a snapshot, the virtual machine NIC might be incorrectly connected to the vSphere Distributed Switch (VDS)**

If you take a snapshot of a virtual machine when the VM NIC is disconnected from a VDS, reverting to that same snapshot, might result in the VM NIC getting connected to the VDS automatically.

This issue is resolved in this release.

- **Distributed Resource Scheduler (DRS) might incorrectly determine that a cluster is imbalanced**

vSphere DRS might incorrectly determine that a cluster is severely imbalanced when the number of failover and non-failover hosts is nearly equal. As a result, DRS frequently triggers vMotion migrations.

This issue is resolved in this release. For the fix to take effect, you must enable the advanced option `ExcludeFailoverHostFromSD` by setting it to `1`. This option excludes any failover hosts from the calculations performed by DRS to detect if a cluster is balanced or not.

- **In complex Active Directory environments, you might fail to log in to the vCenter Server system with a NoPermission error**

In environments with complex or slow Active Directory deployments, the Active Directory users might fail to log in to the vCenter Server system with a `NoPermission` error.

This issue is resolved in this release.

Server Configuration Issues

- **You cannot restart the vpxd service when the KMS certificate is expired or close to the expiration date**

When the KMS certificate is expired or close to the expiration date, you cannot restart the vpxd service and the vCenter Server system upgrade might fail.

This issue is resolved in this release. You must update the KMS certificate before restarting the vpxd service.

Storage Issues

- **vSphere Storage DRS load balancing of multiple thin provisioned disks might take long and block other processes**

If you create multiple thin provisioned disks on a datastore, vSphere Storage DRS might run into an infinite loop while trying to balance loads. As a result, the load balancing operation might block other vSphere Storage DRS processes and affect the performance.

This issue is resolved in this release.

- **vSphere Storage DRS might perform slowly**

Some vSphere Storage DRS tasks, for example providing datastore recommendations, might run slowly. This is due to a timeout in the connection to the Hardware Management Services manager.

This issue is resolved in this release.

- **You might fail to upload any type of file to a datastore**

When you try to upload a file to a datastore, the operation might fail. You might see a 0% progress for the task in the Recent Tasks pane.

This issue is resolved in this release.

- **VMware vSphere Storage DRS might not work properly in environments with linked clone virtual machines**

In environments with linked clone virtual machines or virtual machines that have snapshots, vSphere Storage DRS might not work properly. vSphere Storage DRS might make incorrect recommendations, provide no recommendations for migration, or run migrations between two datastores in an infinite loop. When vSphere Storage DRS migrates a linked clone virtual machine, an incorrect calculation of the disk size might also cause a full copy of the base disk to be created.

This issue is resolved in this release.

- **Reports for storage usage of virtual machines stop refreshing within a few hours after an ESXi host boots**

Reports for storage usage of virtual machines might stop refreshing within a few hours after an ESXi host boots. This issue is due to an underflow error in calculating the storage refresh duration, resulting in unusually long wait times instead of the intended 105-135 minute window.

This issue is resolved in this release. Upgrading to vCenter Server 6.5 Update 3 fixes the timing and re-enables periodic refreshes of storage usage reports.

Backup and Restore Issues

- **A virtual machine might stop responding when you take a snapshot**

When Changed Block Tracking (CBT) is enabled on a virtual machine, the virtual machine keeps track of changing blocks on its disks and requires more memory in the Virtual Machine Executable (VMX), compared to a virtual machine with a disabled CBT. However, VMX does not have dedicated memory limits for CBT and might run out of memory for CBT. As a result, the virtual machine might stop responding.

This issue is resolved in this release.

- **Backup jobs might stop responding if the number of Network Block Device (NBD) parallel sessions exceeds 25**

Backup jobs might stop responding if the number of NBD parallel sessions exceeds 25, due to a concurrency limit.

This issue is resolved in this release.

Licensing Issues

- **If your vSphere edition is lower than vSphere Enterprise Plus, and if you enable vSAN encryption, a license inconsistency in the ESXi host might be exposed**

When you enable vSAN encryption, the Network File Copy functionality checks whether the VM encryption feature is also available for encrypted virtual machines. If your license does not have the VM encryption feature enabled, you cannot clone or migrate encrypted virtual machines.

This issue is resolved in this release.

- **If your vSphere edition is lower than vSphere Enterprise Plus, you cannot synchronize a Content Library or move a host to a cluster**

If your vSphere edition is lower than vSphere Enterprise Plus, you cannot synchronize a Content Library or move a host to a cluster. The operations fail with an exception, such as `NotEnoughLicenses`.

This issue is resolved in this release.

vCenter Server, vSphere Web Client, and vSphere Client Issues

- **User login and logout events might not contain the IP address of the user**

If you log in to a vCenter Server system by using either the vSphere Web Client or the vSphere Client, the login event might display `127.0.0.1` instead of the IP address of the user. In addition, you might not see track of vCenter Single Sign-On configuration changes in the **Events** view.

This issue is resolved in this release. The fix adds a new audit log file in the vCenter Single Sign-On logs. You can also see the new events in the **Monitor > Events** view in the vSphere Web Client and the vSphere Client.

- **When you turn on the pair-wise imbalance check, vSphere DRS might migrate virtual machines even if the cluster seems balanced**

In vCenter Server 6.0 Update 3 and later, if the advanced DRS option CheckPairwiseImbalance is turned on, when DRS detects pair-wise imbalance between two hosts, it continues to do load balancing by migrating virtual machines between the two hosts, even if the cluster seems balanced. A pair-wise imbalance occurs when any two hosts in the cluster have CPU or memory usage difference bigger than the set threshold, which by default is 20%.

This issue is resolved in this release.

- **Disk Bay sensors are categorized as Other devices**

In the vSphere Client, vSphere Web Client, and VMware Host Client, Disk Bay sensors are categorized as Other devices.

This issue is resolved in this release. The fix categorizes the Disk Bay sensors under the Storage category.

vSAN Issues

- **Hardware Compatibility check for Intel VMD controller reports that SCSI controller is not VMware certified**

vSAN health service cannot identify the Intel VMD controller, so it cannot locate the controller in the HCL database. The Hardware Compatibility check reports a SCSI Controller is VMware Certified warning.

This issue is resolved in this release.

- **vSAN disk balance health check incorrectly reports warning**

vSAN disk balance health check might report a warning when the vSAN cluster is balanced.

This issue is resolved in this release.

Tools Issues

- **Update to OVF Tools**

OVF Tools is updated to version 4.3.0 Update 2.

Known Issues

The known issues are grouped as follows.

- [Auto Deploy Issues](#)
- [vCenter Server, vSphere Web Client, and vSphere Client Issues](#)
- [Storage Issues](#)
- [vSAN Issues](#)
- [Known Issues from Earlier Releases](#)

Auto Deploy Issues

- **When you click in the Auto Deploy page on non-English platforms, you might see a warning**

When you click in the Auto Deploy page on non-English platforms, you might see a warning similar to:

`Managing depots is temporarily unavailable. The Image Builder service is down. Try restarting the service to fix the issue.`

Workaround: The services ENABLE AUTO DEPLOY SERVICE and ENABLE IMAGE BUILDER SERVICE are stopped by default. To start them, navigate to **Menu > Auto Deploy > Configure**, select ENABLE AUTO DEPLOY SERVICE and ENABLE IMAGE BUILDER SERVICE to start the services, and refresh the page.

vCenter Server, vSphere Web Client, and vSphere Client Issues

- **The vpxd service might fail to start if certificates in the TRUSTED_ROOTS store exceed 20**

When the certificates in the `TRUSTED_ROOTS` store on the vCenter Server system, which manages the ESXi hosts, pile to more than 20, the vpxd service might fail to start. The vSphere Web Client and vSphere Client display the following error:

`[400] An error occurred while sending an authentication request to the vCenter Single Sign-On server.`

Workaround: This issue is resolved in this release. With this fix, the `TRUSTED_ROOTS` store can support up to 30 certificates in both vCenter Server for Windows and the vCenter Server Appliance.

Storage Issues

- **Deployment of a virtual machine in a vSphere DRS-enabled cluster might fail when there is not enough space to accommodate a thick provisioned virtual machine**

When you deploy a virtual machine in a vSphere DRS-enabled cluster, and you enable thin provisioning, the OVA or OVF deployment might fail, even if there is sufficient space to accommodate the thin provisioned virtual machine. The deployment of a thin provisioned virtual machine succeeds only if enough space is available to accommodate the thick provisioned virtual machine. This issue occurs when you perform a direct deployment to an ESXi host or cluster and when the new virtual machine is deployed from a template in Content Library.

Workaround: Provide enough storage space on the target datastore or choose a different datastore that has enough space to accommodate a thick provisioned virtual machine.

vSAN Issues

- **vSAN health service fails after patching a vCenter Server Appliance configured with a custom port for HTTP and HTTPS**

After patching a vCenter Server Appliance to release 6.5 Update 2 or later, the vSAN health service might fail to start. A message is displayed in the `/var/log/vmware/vsan-health/vmware-vsan-health-service.log`, similar to the following:

```
Failed to log into VC, retrying in 10 seconds
```

This problem occurs when the configuration file for vSAN health service, `/etc/vmware-vsan-health/config.conf`, does not handle custom ports correctly during the patching of the vCenter Server Appliance.

Workaround: Follow the steps in VMware knowledge base article [70731](#).

Known Issues from Earlier Releases

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

Copyright © Broadcom