# VMware vCenter Server 7.0 Update 1c Release Notes

vCenter Server 7.0 Update 1c | 17 DEC 2020 | ISO Build 17327517

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

- **Advanced Cross vCenter vMotion:** With vCenter Server 7.0 Update 1c, in the vSphere Client, you can use the Advanced Cross vCenter vMotion feature to manage the bulk migration of workloads across vCenter Server systems in different vCenter Single Sign-On domains. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and works for both on-premise and cloud environments. Advanced Cross vCenter vMotion facilitates your migration from VMware Cloud Foundation 3 to VMware Cloud Foundation 4, which includes vSphere with Tanzu Kubernetes Grid, and delivers a unified platform for both VMs and containers, allowing operators to provision Kubernetes clusters from vCenter Server. The feature also allows smooth transition to the latest version of vCenter Server by simplifying workload migration from any vCenter Server instance of 6.x or later
- **Parallel remediation on hosts in clusters that you manage with vSphere Lifecycle Manager baselines:** With vCenter Server 7.0 Update 1c, you can run parallel remediation on ESXi hosts in maintenance mode in clusters that you manage with vSphere Lifecycle Manager baselines.
- **Third-party plug-ins to manage services on the vSAN Data Persistence platform:** With vCenter Server 7.0 Update 1c, you can enable third-party plug-ins to manage services on the vSAN Data Persistence platform from the vSphere Client, the same way you manage your vCenter Server system. For more information, see the vSphere with Tanzu Configuration and Management documentation.
- For VMware vSphere with Tanzu updates, see VMware vSphere with Tanzu Release Notes.

## Earlier Releases of vCenter Server 7.0

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

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

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.
For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

## Patches Contained in This Release

This release of vCenter Server 7.0 Update 1c delivers the following patch. See the VMware Patch Download Center for more information on downloading patches.

- Patch for VMware vCenter Server Appliance 7.0 Update 1c

## Patch for VMware vCenter Server Appliance 7.0 Update 1c

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

This patch is applicable to vCenter Server.

| | |
|---|---|
| **Download Filename** | VMware-vCenter-Server-Appliance-7.0.1.00200-17327517-patch-FP.iso |
| **Build** | 17327517 |
| **Download Size** | 5357.1 MB |
| **md5sum** | a3d2bf389e0986e638c7d60529db779d |
| **sha1checksum** | cb21c166e54ba66dd9dadf1ca6f316ece689450f |

**Download and Installation**

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

1. Attach the `VMware-vCenter-Server-Appliance-7.0.1.00200-17327517-patch-FP.iso` file to the vCenter Server CD or DVD drive.

2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:
    - To stage the ISO:
      ```
      software-packages stage --iso
      ```
    - To see the staged content:
      ```
      software-packages list --staged
      ```
    - To install the staged rpms:
      ```
      software-packages install --staged
      ```

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

# Product Support Notices

- Deprecation of SSPI, CAC and RSA
  In a future vSphere release, VMware plans to discontinue support for Windows Session Authentication (SSPI), Common Access Card (CAC), and RSA SecurID for vCenter Server. In place of SSPI, CAC, or RSA SecurID, users and administrators can configure and use Identity Federation with a supported Identity Provider to sign in to their vCenter Server system.

# Resolved Issues

The resolved issues are grouped as follows.



**Auto Deploy Issues**

- **You cannot PXE boot an ESXi host by using vSphere Auto Deploy due to a network error**
  For ESXi hosts with Emulex and Qlogic host bus adapters (HBA), attempts to PXE boot the host by using vSphere Auto Deploy might fail due to a network error. For some Emulex adapters, in the PXE boot console you see a message such as:
  ```
  Could not open net0: Input/output error http://ipxe.org/1d6a4a98'
  Network error encountered while PXE booting.
  Scanning the local disk for cached image.
  If no image is found, the system will reboot in 20 seconds ……
  Could not boot. No such device (http://ipxe.org/2c048087)
  ```

  Emulex HBA adapters that persistently face the issue are:

    - HPE StoreFabric CN1200E-T 10Gb Converged Network Adapter
    - HPE StoreFabric CN1200E 10Gb Converged Network Adapter
    - HP FlexFabric 20Gb 2-port 650FLB Adapter
    - HP FlexFabric 20Gb 2-port 650M Adapter

  For ESXi hosts with QLogic HBAs, attempts to PXE boot the host by using vSphere Auto Deploy do not always fail.

  If the ESX host encounters the issue, in the PXE boot console you see a message such as:
  ```
  Configuring (net0 f4:03:43:b4:88:d0)......
  No configuration methods succeeded (http://ipxe.org/040ee186)
  Network error encountered while PXE booting.
  ```

  The affected Qlogic HBA adapter is HP Ethernet 10Gb 2-port 530T.

  This issue is resolved in this release.

**CIM and API Issues**

- **Remote queries to the SNMP agent on the vCenter Server Appliance fail**

If the SNMP agent on the vCenter Server Appliance runs out of memory, the agent might stop answering queries from remote clients.
In the backtrace, you can see error messages such as:
`2019-11-13T07:16:12.282841+00:00 dk-vcdmng11 snmpd[47594]: 27:load_pci: mmap(-1) failed, Cannot allocate memory`

This issue is resolved in this release.

Guest OS Issues

- **Windows OS customization fails when the original hostname of the Windows OS is longer than 15 bytes**
  If you deploy a virtual machine template with a Windows OS that has a hostname longer than 15 bytes, the guest OS customization fails. In the customization log file `%WINDIR%\Temp\vmware-imc\guestcustutil.log`, you see an error message such as `More data is available`.

  This issue is resolved in this release.

Miscellaneous Issues

- **The VMware Platform Services Controller Health Monitor service, pschealth, intermittently fails and restarts**
  The pschealth service might intermittently fail due to an invalid memory free operation, and restart. You see `core.pschealthd.*` files in the `/storage/core` partition.

  This issue is resolved in this release.

- **The SNMP monitoring tool reports hrMemorySize OID as zero**
  The SNMP monitoring tool might not correctly report the `hrMemorySize OID` as zero in the HOST-RESOURCES-MIB.

  This issue is resolved in this release.

- **File-based backup by using the Virtual Appliance Management Interface and the NFS protocol fails with an error**
  In the Virtual Appliance Management Interface, you might see an error such as `Access Denied` while scheduling a file-based backup of the vCenter Server Appliance by using the NFS protocol. The error appears at the NFS mount point.

  This issue is resolved in this release.

- **If an OVF URL is not accessible by the proxy server in your vCenter Server system, OVF deployment might fail**
  If an OVF URL is not accessible by the proxy server in your vCenter Server system, such as an internal HTTP/S URL in both vCenter Server or ESXi inventory, you might not be able to deploy or export OVF templates.

  This issue is resolved in this release. You can exclude both the OVF Deploy URL domain and the ESX hosts from the proxy server. To exclude ESXi hosts from the proxy settings, in the `/etc/sysconfig/proxy` file you can use CIDR notations, such as `1.2.3.4/24`, in the content library or netmask notations, such as `1.2.3.4/255.255.255.0`. Alternatively, you can use a regex for the domain names, for example: `.*.vmware.com`. Use a regex, `.*.vmware.com`, not wild cards, `*.vmware.com`.

- **In the vSphere Client, you cannot change the log level configuration of the vpxa service after an upgrade of your vCenter Server system**
  In the vSphere Client or by using API, you might not be able to change the log level configuration of the vpxa service on an ESX host due to a missing or invalid Vpx.Vpxa.config.log.level option after an upgrade of your vCenter Server system.

  This issue is resolved in this release. The vpxa service automatically sets a valid value for the Vpx.Vpxa.config.log.level option and exposes it to the vSphere Client or an API call.

Networking Issues

- **Deployment of a vCenter Server Appliance by using port 5480 at stage 2 fails with unable to save IP settings error**
  If you use `https://appliance-IP-address-or-FQDN:5480` in a Web browser, go to the vCenter Server Appliance Management Interface for stage 2 of a newly deployed vCenter Server Appliance, and you configure a static IP or try to change the IP configuration, you see an error such as `Unable to save IP settings`.

  This issue is resolved in this release.

- **The vpxd service fails after replacing the machine SSL certificate with a custom certificate**
  While you replace the machine SSL certificate of you vCenter Server system with a custom certificate, the vpxd service might fail with an error by the Envoy reverse proxy service such as:
  `Envoy rejected update - Error adding/updating listener edge_https_v6: Failed to load certificate chain`
  This issue occurs because Envoy removes new lines from the body of the custom certificate.

  This issue is resolved in this release.

Security Issues

- **You can reset a vCenter Server system root password with an expired password**
  You can reset a vCenter Server system root password with an expired password, although you must not be able to use any of the last 5 passwords.

  This issue is resolved in this release. The fix adds complexity to the password and prevents the use of expired passwords.

- **Update to the Apache Tomcat server**
  The Apache Tomcat server is updated to version 8.5.58.

- **Update of the SQLite database**

The SQLite database is updated to version 3.33.0.

- **Update of Eclipse Jetty in the vSphere Lifecycle Manager**
  Eclipse Jetty in the vSphere Lifecycle Manager is updated to version jetty-9.4.31.v20200723.

- **Update of the Jackson package**
  The Jackson package is updated to versions 2.10.5, 2.11.2.

- **Update to the Spring Framework**
  The Spring Framework is updated to version 4.3.29.

### Server Configuration Issues

- **If vSphere Cluster Service agent virtual machines are placed in datastores protected by the Site Recovery Manager, migration of such datastores fails**
  If you deploy vSphere Cluster Service agent virtual machines on a datastore that is part of an array-based replication protection group, planned migrations of such datastores fail, because the agent VMs do not power off.

  This issue is resolved in this release.

### Upgrade Issues

- **If you run parallel remediation of many clusters in an NSX-T Data Center-enabled environment, some services might fail**
  If you run parallel remediation of many clusters in an NSX-T Data Center-enabled environment by using the vSphere Lifecycle Manager, some health checks might be skipped. During cluster remediation, health checks run at discrete points in the remediation workflow to ensure service health does not degrade. With many remediation jobs running in parallel, some of the health check reports might fail and the health of certain services might not be considered. As a result, such services might fail during or after the remediation.

  This issue is resolved in this release. To prevent the issue, reduce the number of remediation jobs running in parallel.

- **If you use the latest versions of Chrome and Mozilla browsers and your vCenter Server system is of version earlier than 7.0 Update 1, you cannot export interoperability or pre-update check reports**
  In the vSphere Client, after you generate either of the interoperability or pre-update check reports, the **Export** button in the **Product Interoperability** and **Pre-Update Checks** panes does not work.

  This issue is resolved in this release.

- **If your vCenter Server system HTTPS proxy settings require credentials, you cannot upload a software depot by using an HTTP URL**
  If your vCenter Server system HTTPS proxy settings require credentials, updates by using the vSphere Lifecycle Manager might fail, because you cannot upload a software depot by using an HTTP URL.

  This issue is resolved in this release.

- **Updates from vCenter Server 7.0 to 7.0 Update 1 fail with an error for VMware Directory service schema update failure**
  If the domain functional level (DFL) of the VMware Directory schema is 4 and it contains a legacy schema, updates to vCenter Server 7.0 Update 1 from 7.0 fail during the pre-check stage.
  In the `PatchRunner.log` file, you see similar logs:

  ```
  2020-08-07T13:49:37.058092+00:00 info vmdird t@139837142824768: Domain Functional Level (4)
  2020-08-07T13:49:37.058193+00:00 info vmdird t@139837142824768: VmDirKrbInit, REALM (VSPHERE.LOCAL)
  2020-08-07T13:49:37.058319+00:00 info vmdird t@139837142824768: ACL MODE: Legacy
  2020-08-07T13:49:37.058375+00:00 info vmdird t@139837142824768: >>> Schema patch starts <<<
  2020-08-07T13:49:37.088490+00:00 info vmdird t@139837142824768: New schema instance (0x2a9d1b0)
  2020-08-07T13:49:37.119695+00:00 err vmdird t@139837142824768: CoreLogicModifyEntry failed, DN = cn=aggregate,cn=schemacontext, Error (9700), Message
  (BEEntryModify, (9700)((MDB_BAD_VALSIZE: Too big key/data, key is empty, or wrong DUPFIXED size)(objectClasses)))
  2020-08-07T13:49:37.119797+00:00 err vmdird t@139837142824768: InternalModifyEntry: VdirExecutePostModifyCommitPlugins - code(9700)
  2020-08-07T13:49:37.120148+00:00 err vmdird t@139837142824768: VmDirUpdateSubSchemaSubEntry failed, error (9700)
  2020-08-07T13:49:37.120222+00:00 info vmdird t@139837142824768: VmDirPatchLocalSubSchemaSubEntry did not succeed (9700)
  2020-08-07T13:49:37.123389+00:00 err vmdird t@139837142824768: VmDirSchemaPatchViaFile failed, error (9700)
  ```

  This issue occurs mostly in environments where a vCenter Server with an external Platform Services Controller is upgraded from vCenter Server 6.5.x to 6.7.x to 7.0, and then updated to 7.0 Update 1.

  This issue is resolved in this release.

### vCenter Server and vSphere Client Issues

- **In the vSphere Client, you see wrong labels for Privileges of Site Recovery Manager users**
  In the vSphere Client, you see wrong labels for Privileges when setting up Roles for Site Recovery Manager users.

  This issue is resolved in this release.

### vSAN Issues

- **You can provision any entity with a vSAN Host Affinity policy**

The vSAN Host Affinity storage policy option requires VMware validation to ensure proper deployment. However, no restrictions exist to limit the provisioning of entities with the vSAN Host Affinity policy to only such that meet certain criteria. For example, vSAN File Services agent VMs and first-class disks (FCDs) created for Path Selection Plug-in (PSP) applications. This fix makes sure you can use a vSAN Host Affinity policy only in the following scenarios:

1. A vSAN File Services agent virtual machine is provisioned with FileService Host Affinity policy
2. An FCD is provisioned with a non FileService Host Affinity policy
3. Only when `config.vpxd.vsan.hostaffinity.enable=true` and `config.vpxd.vsan.persistenceservice.enable=false`

This issue is resolved in this release.

**vSphere HA and Fault Tolerance Issues**

- **Changes to local user accounts and the root account password are not synced between vCenter Server High Availability nodes**
  In a vCenter Server High Availability environment, creating or modifying local user accounts, or updating the root account password, is not replicated to the passive node.

  This issue is resolved in this release.

**vSphere Lifecycle Manager Issues**

- **A vCenter Server system unexpectedly powers off without a backtrace**
  A vCenter Server system might unexpectedly power off when a thread of the VMware Service Lifecycle Manager service becomes unresponsive due to a system failure or when a process failure, such as a disk I/O error, occurs. However, the VMware Service Lifecycle Manager does not log a specific message for the failure.

  This issue is resolved in this release. The fix enables a reboot instead of a shutdown of the vCenter Server system in case of a system or process failure to make sure you can review logs for the root cause after the reboot.

# Known Issues

The known issues are grouped as follows.



**Upgrade Issues**

- **vCenter Server system upgrades fail in the pre-check stage**
  Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

  ```
  Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200
  Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.
  ```

  You might also see delayed response from the vSphere Client to load the inventory.

  Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs`. Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

# Known Issues from Prior Releases

To view a list of previous known issues, click here.