Hitachi Content Platform

HCP Software Version 9.6.3

HCP Operating System Version 9.6.3

Release Notes

This document contains release notes for Hitachi Content Platform 9.6.3.

RN-RC001-103
March 2024

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Contents

Content Platform 9.6.3 Release notes - Customer

About this document

This document contains release notes for Hitachi Content Platform 9.6.3.

Release highlights

The HCP version 9.6.3 is a maintenance release that, in addition to resolving several issues, adds support for the following appliance components:

- Added support for the 3916 RAID controller card with the HCP G11 appliance. G11 Hardware Setup Tool version 3.1 or later is required to support the 3916 RAID controller.
- Added support for NVIDIA Mellanox ConnectX-4 Lx SFP28 network interface card on the HCP G11 appliance. 25 Gb can be run on both the back-end and the front-end network.

The release also resolves several software issues observed in prior HCP releases:

- Fixed an S-Node retirement issue, where S Node retirement got stuck, with negative file size usage being reported in the SMC.
- Fixed an upgrade issue where online upgrade to v9.6 or later failed in specific rare circumstances of AD settings after the first upgraded node started using newer messaging type.
- Resolved an issue where the SMC reported an error indicating missing Management network IP addresses for nodes that have been retired.
- Resolved an issue that was causing the deletion of empty parent directories to time-out.
- Resolved an issue where arc-deploy could not unmount /tmp/upgrade_root/run when an upgrade restarted after a failed attempt.
- Fixed an issue where DNS failover stopped working after the clusters involved in the replication setup were renamed.
- Resolved an issue where domain/DNS aliases were not updated after cluster rename, causing DNS failover to stop working.
- Resolved an issue where putObject and uploadPart requests were failing against HCP when the supplied requests used Transfer-Encoding: chunked and (an incorrectly calculated) content-length header at the same time.
- Resolved an issue related to management port configuration where the configuration information was not cleaned up after the management port is disabled. This bug that was also causing issues with new VLAN creation.
- Resolved a log spam issue related to retry logic logging immediately on undetermined write results, which caused bloating of the JVM logs.
- Disabled the bash session timeout, which caused SSH sessions to terminate after 15 minutes, resulting in supportability impact.
- Resolved an issue where the replication finishRecovery process on an A/P replication link experienced long delay before completion.
- Resolved a security vulnerability in the PKCS#11 where the ssh-agent in OpenSSH prior to 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution.
- Resolved a security vulnerability in Apache Struts Remote Code Execution.
- Resolved vulnerabilities with HTTP OPTIONS method on port 443 reported by Nessus scan.

Upgrade notes

HCP upgrades can occur with the system either online or offline. During an online upgrade, the system remains available to users and applications. Offline upgrades are faster than online upgrades, but the system is unavailable while the upgrade is in progress.

Observe the following increase in upgrade times:

- Online upgrades to HCP v9.6.3 from versions other than HCP v9.4.4: Upgrades may take up to two additional hours per node for HCP systems using cloud or S Series storage . The upgrade time estimate may vary based on the number of objects in the HCP system and how active the HCP system is.
- Offline upgrades to HCP v9.6.3 from versions other than HCP v9.4.4: Upgrades may take an additional 1.5 hours to complete. There is no increase in upgrade time for HCP systems that have no S Series or cloud storage in use as long as all nodes in the HCP system are being upgraded at the same time.

Note: This increase in upgrade time occurs only on an HCP v9.6.3 upgrade. It will not be repeated if S Series or cloud Storage is added after upgrading to HCP v9.6.3 or if an HCP system is upgraded from v9.6.3 to a later version.

Note: During an online upgrade, data outages might occur as each node is upgraded. Whether data users are affected by an outage depends on the ingest tier Data Protection Level (DPL) setting specified in the service plan that's assigned to the applicable namespace. No data is lost during a data outage, but users may experience some data-access interruptions.

When upgrading to this release from a version prior to HCP version 9.6, the boot partition on the OS disk gets resized from 199 MB to 499 MB, while the swap partition size is reduced to 3.7 GB.

After upgrading to this release, new password requirement rules apply to a newly created password when the Install user account’s password is changed next time. The password must be 14 characters or longer, and must include characters from 4 groups of characters. For more information, see the installation manual.

In VM environments, the OS disk can now be either 64 GB or 32 GB. New installations should utilize 64 GB OS disk, but any existing system with 32 GB OS disk can be upgraded to this release.

Upgrades to HCP version 9.4.0 or later will fail if any of the namespaces have HSwift protocol enabled. Disable HSwift protocol on the relevant namespaces before upgrading. Support for HSwift protocol has ended with HCP 9.3.0.

Upgrades to version 9.2.1 or later will fail if any service plans exist that have SMTP enabled and use direct write to HCP S Series Nodes as the primary ingest tier. Please modify these service plans before upgrading to version 9.2.1 or later. For more information, please contact your authorized HCP service provider.

You can upgrade an HCP system to version 9.x only from version 8.x. You cannot downgrade HCP to an earlier version.

You must have at least 32 GB of RAM per node to use new software features introduced in HCP version 9.x. While you can upgrade an HCP system to version 9.x with a minimum of 12 GB of RAM per node and receive the patches and bug fixes associated with the upgrade, the system cannot use the new software features in the release. Inadequate RAM causes performance degradation and can negatively affect system stability. If you have less than 32 GB RAM per node and would like to upgrade to this release, contact your Hitachi Vantara account team.

HCP Data Migrator is no longer supported starting with HCP version 9.4.0. HCP Data Migrator was deprecated as of HCP release 9.2.1.

Supported limits

HCP supports the limits listed in the following tables.

Hardware

Table 1 Hardware support limits

Hardware	Support limit
Maximum number of general access, G Series Access Nodes	80
Maximum number of HCP S Series Nodes	80

KMIP server

Table 2 KMIP server limits

Hardware	Support limit
Maximum number of KMIP servers	8

Logical storage volumes

Table 3 SAN-attached (SAIN) HDD systems

Logical volume	Support limit
Maximum number of SAN logical storage volumes per storage node	63
Maximum logical volume size for SAN LUNs	15.999 TB

Table 4 Internal storage (RAIN) HDD systems

Internal storage	Support limit
Maximum number of logical storage volumes per storage node RAIN	4
Maximum logical volume size on internal drives	HDD capacity dependent

Table 5 All-SSD systems (internal storage or SAN-attached)

Internal storage	Support limit
Number of SSDs per storage node	12 (front-cage only)
Maximum logical volume size on internal drives	SSD capacity dependent
Maximum number of SAN logical storage volumes per storage node (when SAN is attached to system)	63
Maximum logical volume size for SAN LUNs (when SAN is attached to system)	15.999 TB

Table 6 HCP VM systems — VMware ESXi

HCP VM systems — VMware ESXi	Support limit
Maximum number of logical storage volumes per VM storage node	1 OS LUN, 59 Data LUNs
Maximum logical volume size	15.999 TB

Table 7 HCP VM systems — KVM

HCP VM systems — KVM	Support limit
Maximum number of logical storage volumes per VM storage node	1 OS LUN Data LUNs: Limited by the number of device slots available for LUNs in the VirtIO-blk para-virtualized storage back-end, which depends on the number of other devices configured for the guest OS that also use the VirtIO-blk back-end. In a typical HCP configuration, 17 slots are available.
Maximum logical volume size	15.999 TB OS LUN

Table 8 Data storage

Data storage	Support limit
Maximum active erasure coding topologies	1
Maximum erasure coding topology size	6 (5+1) sites
Minimum erasure coding topology size	3 (2+1) sites

Data storage	Support limit
Maximum total erasure coding topologies	5
Maximum number of objects per storage node	Standard non-SSD disks for indexes: 800,000,000 SSD for indexes: 1,250,000,000
Maximum number of objects per HCP system	64,000,000,000 (80 nodes times 800,000,000 objects per node) If using 1.9 TB SSD drives: 100,000,000,000 (80 nodes times 1,250,000,000 objects per node)
Maximum number of directories per node if one or more namespaces are not optimized for cloud	1,500,000
Maximum number of directories per node if all namespaces are optimized for cloud	15,000,000
Maximum number of objects per directory	By namespace type: ▪ HCP namespaces with unbalanced directory setting: no restriction ▪ HCP namespaces with balanced directory setting: 30,000,000
Maximum object size by protocol	▪ HTTP: About 2 TB (2,194,719,883,008 bytes) ▪ Hitachi API for Amazon S3: • Without multipart upload: About 2 TB (2,194,719,883,008 bytes) • With multipart upload: 5 TB ▪ WebDAV: About 2 TB (2,194,719,883,008 bytes) ▪ CIFS: 100 GB ▪ NFS: 100 GB
Maximum total KM servers	8
Hitachi API for Amazon S3: Minimum size for parts in a complete multipart upload request (except the last part)	1 MB
Hitachi API for Amazon S3: Maximum part size for multipart upload	5 GB

Data storage	Support limit
Hitachi API for Amazon S3: Maximum number of parts per multipart upload	10,000
Maximum number of replication links	20 inbound, 5 outbound
Maximum number of tenants	1,000
Maximum number of namespaces	10,000
Maximum number of namespaces with the CIFS or NFS protocol enabled	50

Table 9 User groups and accounts

User groups and accounts	Support limit
Maximum number of system-level user accounts per HCP system	10,000
Maximum number of system-level group accounts per HCP system	100
Maximum number of tenant-level user accounts per tenant	10,000
Maximum number of tenant-level group accounts per tenant	100
Maximum number of users in a username mapping file (default tenants only)	1,000
Maximum number of SSO-enabled namespaces	~1200 (SPN limit in Active Directory)

Table 10 Custom metadata

Custom metadata	Support limit
Maximum number of annotations per individual object	10
Maximum non-default annotation size with XML checking enabled	1 MB
Maximum default annotation size with XML checking enabled	1 GB
Maximum annotation size (both default and non-default) with XML checking disabled	1 GB
Maximum number of XML elements per annotation	10,000
Maximum level of nested XML elements in an annotation	100

Custom metadata	Support limit
Maximum number of characters in the name of custom metadata annotation	32
Maximum form size in POST object upload	1,000,000 B
Maximum custom metadata size in POST object upload	2 KB
Maximum number of SSO-enabled namespaces	~1200 (SPN limit in Active Directory)

Table 11 Access control lists

Access control lists	Support limit
Maximum size of access control entries per ACL	1,000 MB

Table 12 Metadata query engine

Metadata query engine	Support limit
Maximum number of content classes per tenant	25
Maximum number of content properties per content class	100
Maximum number of concurrent metadata query API queries per node	5

Table 13 Network

Network	Support limit
Maximum number of user-defined networks (virtual networks) per HCP system	200
Maximum downstream DNS servers	32
Maximum certificates and CSR per domain	10

Table 14 Storage tiering

Storage tiering	Support limit
Maximum number of storage components	100
Maximum number of storage pools	100

Storage tiering	Support limit
Maximum number of tiers in a service plan	5

Table 15 Miscellaneous

Miscellaneous	Support limit
Maximum number of HTTP connections per node	255
Maximum number of SMTP connections per node	100
Maximum number of attachments per email for SMTP	50
Maximum aggregate email attachment size for SMTP	500 MB
Maximum number of access control entries in an ACL	1,000
Maximum number of labeled retention holds per object	100

Supported browsers and platforms

The following sections list browsers and platforms that are qualified for use with HCP.

Browsers

The table below lists the web browsers that are qualified for use with the HCP System Management, Tenant Management, and Search Consoles and the Namespace Browser. Other browsers or versions may also work.

Note: HCP 9.4.0 and later versions no longer support Microsoft Internet Explorer® 11 because Microsoft no longer supports that browser. As a replacement, Microsoft Edge has been added as a supported browser in addition to Mozilla Firefox and Google Chrome.

Browser	Client Operating System
Microsoft Edge	Windows
Mozilla Firefox®	Windows HP-UX IBM AIX Red Hat Enterprise Linux Sun Solaris

Browser	Client Operating System
Google Chrome®	Windows HP-UX IBM AIX Red Hat Enterprise Linux Sun Solaris
*The Consoles and Namespace Browser work in Internet Explorer only if ActiveX is enabled. Also, the Consoles work only if the security level is not set to high.	

Note: To correctly display the System Management Console, Tenant Management Console, and Namespace Browser, the browser window must be at least 1,024 pixels wide by 768 pixels high.

Platforms for HCP VM

HCP VM runs on these platforms:

- VMware ESXi 6.5 U1 and U2
- VMware ESXi 6.7 U1, U2, and U3
- VMware ESXi 7.0 (qualified on hardware version 17)
- VMware vSAN 6.6
- VMware vSAN 6.7
- VMware vSAN 7.0
- KVM — qualified on CentOS 7 and Fedora Core 29. For relevant support, configuration, installation, and usage information, see *Deploying an HCP-VM System on KVM* (MK-94HCP009-06).

Third-party integrations

The following third-party applications have been tested and proven to work with HCP. Hitachi Vantara does not endorse any of the applications listed below, nor does Hitachi Vantara perform ongoing qualification with subsequent releases of the applications or HCP. Use these and other third-party applications at your own risk.

Hitachi API for Amazon S3 tools

These tools are qualified for use with the Hitachi API for Amazon S3:

- CloudBerry Explorer (does not support multipart upload)
- CloudBerry Explorer PRO (for HCP multipart upload, requires using an Amazon S3 compatible account instead of a HCP account; for CloudBerry internal chunking, requires versioning to be enabled on the target bucket)
- S3 Curl
- S3 Browser

Mail servers

These mail servers are qualified for use with the SMTP protocol:

- Microsoft Exchange 2010 (64 bit)
- Microsoft Exchange 2013
- Microsoft Exchange 2016

NDMP backup applications

These NDMP backup applications are qualified for use with HCP:

- Hitachi Data Protection Suite 8.0 SP4 (CommVault® Simpana® 8.0)
- Symantec® NetBackup® 7 — To use NetBackup with an HCP system:
    - Configure NDMP to require user authentication (that is, select either the Allow username/pwd authenticated operations or Allow digest authenticated operations option in the NDMP protocol panel for the default namespace in the Tenant Management Console).
    - Configure NetBackup to send the following directive with the list of backup paths:

```
set TYPE=openPGP
```

Windows Active Directory

HCP is compatible with Active Directory on servers running Windows Server 2012 R2 or Windows Server 2016. In either case, all domain controllers in the forest HCP uses for user authentication must minimally be at the 2012 R2 functional level.

RADIUS protocols

HCP supports the following RADIUS protocols:

- CHAP
- EAPMD5

- MSCHAPv2
- PAP

System Monitoring

The following system monitoring and alerting third-party tools are integrated with HCP and expose their end-points for third-party monitoring, dashboarding, and alerting solutions:

- Prometheus v2.37.0:
  - Prometheus API documentation: https://prometheus.io/docs/prometheus/2.37/querying/api/
  - Qualified visualization of Prometheus metrics with Grafana v9.4
- Alertmanager (Prometheus Alerting): Alertmanager v0.24.0

Supported hardware

The following sections list hardware that is supported for use in HCP systems.

> **Note:** The lists of supported hardware are subject to change without notice. For the most recent information on supported hardware, contact your HCP sales representative.

Supported servers

These servers are supported for HCP systems with internal storage:

- HCP G11 (D52BQ-2U)
- HCP G10 (D51B-2U)

These servers are supported for HCP SAN-attached systems with internal storage:

- HCP G11 (D52BQ-2U)
- HCP G10 (D51B-2U)

Server memory

At least 32 GB of RAM per node is needed to use new software features introduced in HCP 9.x. An HCP system can be upgraded to version 9.x with a minimum of 12 GB of RAM per node, and receive the patches and bug fixes that come with the upgrade, but the system cannot use the new software features. Inadequate RAM causes performance degradation and can negatively affect system stability.

If you have less than 32 GB RAM per node and would like to upgrade to HCP 9.x, contact your Hitachi Vantara account team.

Supported storage platforms

These storage platforms are supported for HCP SAIN systems:

- Hitachi Virtual Storage Platform
- Hitachi Virtual Storage Platform G200
- Hitachi Virtual Storage Platform G400
- Hitachi Virtual Storage Platform G600
- Hitachi Virtual Storage Platform G1000
- Hitachi Virtual Storage Platform G1500
- Hitachi Virtual Storage Platform 5100
- Hitachi Virtual Storage Platform 5100H
- Hitachi Virtual Storage Platform 5200
- Hitachi Virtual Storage Platform 5200H
- Hitachi Virtual Storage Platform 5500
- Hitachi Virtual Storage Platform 5500H
- Hitachi Virtual Storage Platform 5600
- Hitachi Virtual Storage Platform 5600H
- Hitachi Virtual Storage Platform E590
- Hitachi Virtual Storage Platform E790
- Hitachi Virtual Storage Platform E990
- Hitachi Virtual Storage Platform E1090

Supported back-end network switches

The following back-end network switches are supported in HCP systems:

- Alaxala AX2430
- Arista 7020SR-24C2-R
- Cisco® Nexus® 3K- C31128PQ-10GE
- Cisco® Nexus® 3K-C31108PC-V
- Cisco® Nexus® 5548UP
- Cisco® Nexus® 93180YC-FX
- Cisco® N9K-C93180YC-FX3
- Cisco® 5596UP
- ExtremeSwitching™ VDX® 6740
- ExtremeSwitching™ 210
- ExtremeSwitching™ 6720 - SAIN systems only
- HP 4208VL

- Ruckus ICX® 6430-24
- Ruckus ICX® 6430-24P HPOE
- Ruckus ICX® 430-48

Recommendations for HCP back-end network switch configuration

If an HCP system is using customer-supplied and managed back-end network switches, as in the case for an HCP system hosted on VMware, and the back-end network configuration requires IGMP snooping, configure the back-end as follows:

- **Set the Querier's IP address**: **The Querier's IP address should be set to an IP address within the subnet of the HCP back-end network**. This is required for the Querier to detect and manage multicast group membership properly.

Supported Fibre Channel switches

The following Fibre Channel switches are supported for HCP SAIN systems:

- Brocade 5120
- Brocade 6510
- Cisco MDS 9134
- Cisco MDS 9148
- Cisco MDS 9148S

Supported Fibre Channel host bus adapters

These Fibre Channel host bus adapters (HBAs) are supported for HCP SAIN systems:

- Emulex® LPe 32002-M2-Lightpulse

  (for supported firmware and boot BIOS versions, refer to the G11 Hardware Tool set)
- Emulex® LPe 11002-M4

  (firmware version 2.82a4, boot BIOS 2.02a1)
- Emulex® LPe 12002-M8

  (firmware version 1.10a5, boot BIOS 2.02a2)
- Emulex® LPe 12002-M8 (GQ-CC-7822-Y)

  (firmware version 1.10a5, boot BIOS 2.02a2)
- Hitachi FIVE-EX 8Gbps

  (firmware version 10.00.05.04)

Issues resolved

Issues resolved in this release

The following table lists the issue resolved in HCP 9.6.3.

Reference Number	SR Number	Description
HCP-47099	04189673, 04341593	Resolved an issue related to management port configuration where the configuration information was not cleaned up after the management port is disabled. This bug also caused issues with new VLAN creation.
HCP-47102	04176117, 03964645, 03398188	Resolved an issue where domain/DNS aliases were not updated after renaming a cluster, which caused DNS failover to stop working as expected.
HCP-47103	—	Resolved an issue where HCP was not returning a valid `versionId` element for `listObjectVersions` requests on versioning-disabled buckets.
HCP-47105	—	Resolved an issue where encrypt Cloud Pools options disappear and show only encryption with local key management option while updating the service plan name.
HCP-47106	—	Resolved an issue where incorrect message content was added to the replication logs related to replication `linkId`.
HCP-47107	—	Resolved an issue that caused the deletion of empty parent directories to time out.
HCP-47108	03210417, 03226903	Resolved a log spam issue related to retry logic logging immediately on undetermined write results, which caused bloating of the JVM logs.
HCP-47109	—	Removed spring-test v3.0.7 jar from HCP because there were multiple security vulnerabilities reported with the Spring v3.0.7 framework.
HCP-47111	—	Resolved an issue where `putObject` and `uploadPart` requests were failing against HCP when the supplied requests used Transfer-Encoding: chunked and an incorrectly calculated content-length header at the same time.
HCP-47112	—	Resolved an issue where disk cache is left Enabled on upgrades from releases prior to HCP 9.6.

Reference Number	SR Number	Description
HCP-47113	04262089, 03117669	Resolved an issue where the replication `finishRecovery` process on an A/P replication link experienced a long delay before completion.
HCP-47114	03020014, 02989847, 03020014	Resolved an issue where arc-deploy could not unmount /tmp/upgrade_root/run when an upgrade restarted after a failed attempt.
HCP-47115	02903116	Resolved a security vulnerability where HCP responded to an HTTP OPTIONS request on port 443 to which it was not supposed to respond.
HCP-47116	02852874, 02142039, 04270639/04226729	Resolved an issue where the SMC reported an error on missing Management network IP addresses for nodes that were retired.
HCP-47117	00749017	Resolved an issue where the A/P replication link schedule did not adjust for systems located in different time zones.
HCP-47118	04176117	Resolved an issue where DNS failover stopped working after the clusters involved in the replication set up were renamed.
HCP-47119	04140600	Resolved an issue involving multi-part objects (MPO) in replication environment, which caused replication lag due to `MissingMPOMarkerException`.
HCP-47121	—	Resolved an issue where `Cluster_ssh.py` output collected excessive length of output that impacted support users.
HCP-47141	—	Disabled the bash session timeout, which caused ssh sessions to terminate after 15 minutes, resulting in usability impact.
HCP-47142	04371415	Resolved an issue where using the namespace user interface (UI) to create folders and subfolders that have a space in the their names caused duplicate folder names to appear in the UI with percent-encoded characters.
HCP-47242	04345095	Resolved an upgrade issue where, online upgrade to v9.6 or later failed in specific rare circumstances of Active Directory settings after the first upgraded node started using a newer messaging type.

Reference Number	SR Number	Description
HCP-47313	—	Resolved an installation issue on G10 systems with rear cage SSDs.
HCP-47370	03753667, 04301585, 04339063, 04343774, 04404666 04426996	Resolved an S Node retirement issue, where S Node retirement got stuck, with negative file size usage being reported in the SMC.
HCP-47371	04336433	Resolved an issue where node status API could not return the correct response code when a cluster was in read-only mode and Metadata manager either was not running or was spinning trying to create a new map.
HCP-47748	—	Audit daemon (auditd.service) will be disabled on new HCP installations and upgrades to HCP v9.6.3.

Common Vulnerabilities and Exposures (CVE) Records and other security vulnerabilities resolved in this release (9.6.3)

CVE Record Number	Hitachi Vantara reference number	Description
CVE-2023-38408	HCP-47097	The PKCS#11 feature in ssh-agent in OpenSSH prior to 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system.
CVE-2023-50164	HCP-47144	An attacker can manipulate file-upload parameters to enable paths traversal. Under some circumstances, this can lead to uploading a malicious file that can be used to perform Remote Code Execution.
None	HCP-47115	Resolved a security vulnerability where HCP responded to HTTP OPTIONS request on port 443, when it is not supposed to respond.

Compatibility issues introduced in HCP 8.2 or later

The following table lists the compatibility issues introduced in HCP v8.2 or later. The issues are listed in ascending order by reference number.

Ref. number	Description	Version introduced in
HCP-33074 HCP-35329	In HCP v8.2, the HCP software was upgraded to Jetty v9. The upgrade introduces several security enhancements that might impact some deployments: ▪ HCP no longer supports SSL v1, v2, and v3 protocols. ▪ HCP conforms more closely to RFC 7230, and no longer allows header folding.	HCP v8.2
HCP-33583	HCP now requires that the x-amz-date header value is within 15 minutes of when HCP receives the Hitachi API for Amazon S3 request.	HCP v8.2
HCP-33672	HCP now validates `x-amz-date` headers on appropriate Hitachi API for Amazon S3 requests.	HCP v8.2

Ref. number	Description	Version introduced in
HCP-35286	HCP now sends the severity of the EventID/ messages such as NOTICE, WARNING or ERROR to Syslog servers.	HCP v8.1
HCP-37063	Use case of a namespace, with SMTP enabled directly writing to HCP S Series Node, is no longer supported.	HCP v8.2
HCP-37858	Use case of a namespace, with SMTP enabled directly writing to HCP S Series Node, is no longer supported.	HCP v9.1
HCP-43818	Certain third-party tools and SDK solutions that connect to HCP through HTTPS may not support TLS v1.3. With the release of HCP 9.4, for example, one such tool was found to be the AWS Command Line Interface (AWS CLI). Similarly, HCP Anywhere 4.5.4 does not yet support TLS 1.3. Therefore, setting HCP to TLS 1.3 minimum stops HCP-AW communications until HCP is changed back to use TLS 1.2 as maximum TLS level. A future release of HCP Anywhere is expected to add support for TLS 1.3; please refer to the appropriate release notes of HCP Anywhere for further information. Before turning on TLS 1.3 in HCP, make sure that the tools and SDKs used to connect to HCP through HTTPS connection do support TLS v1.3.	HCP v9.4
HCP-45026	The version Id tag is missing from the results when trying to list all objects and their versions on a namespace where versioning is not enabled.	

Known issues

The next table lists the known issues in the current release of HCP. The issues are listed in order by reference number. Where applicable, the service request number is also shown.

Reference Number	SR Number	Description
HCP-45870	04048623	After performing an add new nodes procedure in a cluster with VLANs configured for replication, the cluster might enter a read-only state because the HCP software stack fails to start on the newly added nodes.

Reference Number	SR Number	Description
HCP-45680	03964972, 04105209	The MQE query can exhaust the memory resources of the Metadata Query Engine on an IPL2 cluster.
HCP-45003	—	When upgrading to HCP 9.4 version or later from previous HCP versions that are configured with Active Directory (AD), the `sAMAccountName` attribute value of the HCP computer account does not comply with Microsoft requirements (that is, the attribute value is expected to end with $ symbol at the end; however, currently it is present at the beginning of the attribute value). The `sAMAccountName` attribute value does comply with Microsoft requirements on newly installed HCP 9.4 clusters. To comply with the Microsoft requirement on upgraded clusters, customers need to disconnect their HCP system from AD and then reconnect; this process will update the `sAMAccountName` attribute value to comply with the requirement.
HCP-44817	—	The HCP G11 node power supply might trigger a false alarm, indicating `Power supply Power Supplies has triggered an alarm; status: No redundancy.` As a possible workaround, an upgrade of the BMC firmware supported by HCP G11 might resolve the issue.
HCP-44325	03644695	Replication progress may slow down when an HCP cluster is unable to acquire an open file resource because the open file limit has been reached on the cluster.
HCP-43908	—	After a ZCF failover occurs in a SAN-attached HCP cluster, the System Management Console (SMC) Hardware page is not accessible for approximately 5 minutes. After that time, the page should become available.
HCP-43527	03422907	If outbound traffic is blocked while incoming traffic continues to flow, a transmission time-out problem can occur because the bonding driver `arp_validate` setup does not detect half-broken links. This results in backend network communication problems.
HCP-43479	03402060	During log rotation, `arc-rotate` can stop (kill) JVM if log files to be rotated are open.

Reference Number	SR Number	Description

HCP-43284	—	In some circumstances, an offline upgrade might fail because the HCP shutdown process cannot unmount an encrypted archive volume. If this failure occurs, consult Hitachi VantaraSupport.
		An offline upgrade failure adds the following two lines to the HCP logs:
		`Standard ERROR for 'dmsetup remove --force archive001-crypt':`
		`device-mapper: remove ioctl on archive001-crypt  failed: Device or resource busy`

HCP-43082	03422540	The `arc-deploy` during finalize migration might fail halfway if a node roll occurs at the same time.
HCP-42673	—	When a node recovery service procedure is performed on a VM cluster with a dedicated database volume, and volumes are preserved during installation, the service procedure does not use the dedicated database volume for database location.
HCP-42516	—	A corrupt Samba daemon configuration file and a failed Active Directory join might cause the HCP system services to continuously restart with an `NT_STATUS_NO_MEMORY` error.
HCP-41176	03131048, 03141801, 03171024	HCP running on a G11 server can raise a false-positive alert about the power supply, CPU, or disk drives.
HCP-40505	—	Manually started execution of a service is not persistent. It can be interrupted by the scheduled service or a node event such as a reboot.
HCP-39876	02673882	In a SAN-attached HCP environment, storage addition procedure may fail, indicating that the procedure fails because of a device mapper name of mpathb (or other mpath device) cannot be formatted.
HCP-39798	02639142	Solr does not create proper indexing when user ingests a custom metadata containing format other than "Pretty formatted XML." Therefore, annotations with a single line of XML are not parsed properly when doing phrase searches.

Reference Number	SR Number	Description
HCP-39465	—	Objects cannot be deleted using the namespace browser when logged in as an anonymous user. Log in as an authenticated user to delete objects when using the namespace browser.

HCP-38408	02155007	ntpd tries to bind to usb0 network interface on HCP 9.x G11 system and causes time synchronization issues.
		Workaround: On each node, prevent the driver from loading by denylisting in /etc/modprobe.d/aos.conf (that is, add/append the following lines in /etc/modprobe.d/aos.conf:
		`blacklist cdc_ether`
		`blacklist usbnet`

HCP-38155	02090989	Resetting advanced settings for an HCP S Series storage component does not work.
HCP-38048	—	Service clearPolicyState does not clear rows that have no matching `external_file` entries.
HCP-37851	—	Starting with release HCP 8.2, all units of systemd-tmpfiles service log errors messages in /var/log/messages on a daily periodicity. The error log messages are similar to the following: systemd-tmpfiles[29354]: [/usr/lib/tmpfiles.d/mdadm.conf:1] Line references path below legacy directory /var/run/, updating /var/run/mdadm → /run/mdadm; please update the tmpfiles.d/ drop-in file accordingly. Initial investigation suggests that these error messages cause no functional error symptoms in HCP.
HCP-37810	—	When provisioning rear-cage SSD to the HCP cluster on a subset of nodes in a SAN-attached G10 or G11 configuration, the service procedure tries to add rear-cage SSD on both nodes that comprise a Zero-Copy-Failover (ZCF) pair, even if one of those nodes does not have rear-cage SSD to be provisioned. This leads to error in the service procedure. As a work-around, ensure that you provision rear-cage SSDs either for both nodes that comprise a ZCF pair, or simultaneously for all nodes in the cluster.

Reference Number	SR Number	Description
HCP-37778	—	After upgrade of an HCP system is completed, the System Management Console Hardware page may display Initializing status for some of the logical volumes. This is the result of the device SMART error log containing records of error. Please contact Hitachi Vantara technical support to identify the error condition and the corrective action to resolve the symptom.
HCP-37754	—	HCP installed in an ESXi environment may display the following FSTRIM error message on the System Management Console: `Failure encountered attempting to trim volumes on nodes:`, and an error with Event ID 2818 is listed in the error log under Major Events. Please contact Hitachi Vantara customer support if you encounter this error message.
HCP-37753	—	HCP system goes in read-only state because of node rolls due to metadata manager not starting up. The system might even appear to be unstable.. **Workaround:** Reboot the system.
HCP-37696	01612339	MQE shard / solr core balancing doesn’t function as desired for IPL=2 and causes incomplete query results.
HCP-37426	—	Attempting to perform DELETE and PUTCOPY simultaneously on an object results in "Non-replicating Irreparable objects detected" error message in SMC of HCP.
HCP-37381	—	AWS S3 protocol in race condition allowed both directory and file objects created with same pathname. Unlike AWS, HCP has a concept of directories. So the upper level directory cannot be also a file.
HCP-37342	—	An unexpected duplicate row in the per-object metadata table will cause node outages until the duplicate row is removed.
HCP-37335	02509892	HCP product installation procedure may fail with the following error message if there is a USB drive or external DVD drive connected to the system when running the installation wizard: umount: /dev/sr0: umount failed: Invalid argument.

Reference Number	SR Number	Description
		This may occur in both VM and appliance configurations. Please disconnect all unnecessary USB drive and external DVD drives from the system, and retry the installation procedure,
HCP-36798	01709881	SNMP returns the incorrect replication link name **Workaround:** Use the HCP Management API to return the correct replication link name.
HCP-36744	—	In rare circumstances, when HCP G11 operating system is installed on a node, the installation process may hang during making filesystems. This has typically been observed in SAN-attached configurations. This symptom occurs when HCP G11 detects that there appears to already be a filesystem on the volume, and the filesystem creation command is waiting for user input, but the prompt output by that command is not displayed on the console. If you are certain that the filesystem formatting procedure can continue (i.e., the volumes are mapped correctly, and all data on the volume can be destroyed), you can type in `yes` and press Enter, which should allow the procedure to continue.
HCP-36632	01547564	Multipart upload fails in the FileOpenForWriteIndex.suspendAndSwap function and returns an `Attempt to suspend and swap a multipart upload file handle` error.
HCP-36001	01410508	Node recovery during an online upgrade procedure targets a healthy node.
HCP-35089	01426836	Zero-copy failover failback might leave behind stall mount points.
HCP-34982	—	In the HCP Search Console UI, the login ID changes to null and a subsequent search returns `500 Error: Internal server error`. When you open the Tenant Management Console from the System Management Console, initiate a search by logging in to the Search Console with your system-level credentials, and either refresh the page or click the search button, the following events occur: ▪ You are returned to the login page. ▪ The login ID changes to null.

Reference Number	SR Number	Description
		If you log in to the Search Console again with your tenant-level credentials and initiate a search, the query returns the following error message: `500 Error: Internal server error` **Workaround:**Set the Log users out if inactive for more than value to be the same on the System Management Console and Tenant Management Console. You can configure this value on the SMC > Security > Console tab.
HCP-34764	01309564	After disabling CIFS on an HCP namespace, the Windows client connection remains active, and objects are written to the root (/) file system
HCP-34516	01312806, 01310161	Overflowed, thin-provisioned block storage might cause data loss. **Workaround:** Do not over provision dynamic pools.
HCP-34515	01312806	Major capacity of the `/var` file system contains log downloads.
HCP-34388	01224371	When a zero-copy-failover partner node reboots after a failover, the metadata query engine does not recover. **Workaround:** Edit the following files: ▪ In the `/opt/arc/solr/solr/solr.xml` file, add the shards that are on the standby volumes. ▪ In the `/opt/arc/solr/solr/cores` file, create symlinks that point to the shards on the standby volumes.
HCP-34207	—	Faulty SSD drives can cause a failure when adding a new SSD volume to HCP.
HCP-34203	—	Capacity calculations and UI display are inconsistent between HCP and HCP S Series Node.
HCP-33980	—	Some metadata headers are processed inconsistently between AWS S3 and HCP.
HCP-33541	—	Active/passive replication link schedule does not adjust for systems located in different time zones.

Reference Number	SR Number	Description
HCP-32957	—	Metadata query engine with sort option causes Apache Solr Java Virtual Machine to run out of memory.
HCP-32848	—	Delete old database procedure hangs. When administering namespaces with 100,000 objects or more, the Delete Old Database procedure is known to run indefinitely and display #, even though the deletion has completed.
HCP-32555	00294339	Watchdog timer causes premature soft lockup panic.
HCP-32486	—	The Active Directory allowlist filter is removed when the HCP System Management Console fails to update settings.
HCP-32164	—	Unable to change the name of an HCP S Series component in the HCP System Management Console.
HCP-32018	00533224	Migration hangs and produces inconsistent status information.
HCP-31529	—	System restart fails after changing management network configuration. The HCP system should restart each time a change is made to the management network configuration, but after enabling the management network for the first time the HCP system does not restart again from changes made to management network configuration.
HCP-31499	—	Inconsistent case sensitivity for Hitachi API for Amazon S3 multipart upload query parameters. Case sensitivity is inconsistent among the query parameters used with S3 compatible API requests related to multipart uploads. For example, the uploadId query parameter used in requests to upload a part is not case sensitive, while the uploadId query parameter used in requests to list the parts of a multipart upload or complete or abort a multipart upload is case sensitive.
HCP-31488	—	System restart due to unavailable node not receiving management network IP address.

Reference Number	SR Number	Description
		If a node is unavailable when the management network is enabled, the node does not receive the management network IP address. If any other change is made to the management network, the HCP system shuts down so the node can receive the management network IP address. **Workaround:** Only enable the management network when all nodes are available.
HCP-31431	—	Links in a geo-protection replication topology can be added to replication chain. Geo-protection replication chains are not supported. If a system in the geo-replication topology becomes unavailable, the geo-protected systems outside of the topology could experience data unavailability
HCP-31112	01124247	Objects left in "VALID, UNREPLICATABLE_OPEN" state and cannot be cleaned up by running garbage collection.
HCP-30958	—	DNS failover fails due to domain name change in active/passive replication link. If a system is in an active/passive replication link and has its domain name changed, the replica system does not receive the updated domain name which causes DNS failover to fail. **Workaround:** After you change the domain name for the primary system, update any setting on the tenant overview page to replicate the new domain name.
HCP-30058	—	AWS S3 500 Internal Server Error due to double slash (//) in object name If an object has a double slash (//) in its object name and the object is ingested using HS3, HCP returns a HTTP 500 internal server error.
HCP-30018	HDS04030240	Namespace browser cannot load directory due to ASCII characters in object name. The namespace browser cannot display the contents of a directory that contains an object with any of the following ASCII characters in its name: %00-%0F, %10-%1F, or %20.

Reference Number	SR Number	Description
HCP-29645	HDS03709359	AD falsely report missing SPNs due to replication topology with tenant or namespaces on custom network. In a replication topology where systems have full SSO support, HCP may incorrectly report missing SPN errors for replicating tenants and namespaces that are using a custom network with a non-default domain name.
HCP-29301	HDS03709359	Database connections exhausted On high-load HCP systems that are balancing metadata, nodes can restart due to exceeding the database connection limit.
HCP-25602	00496802	While the Migration service is running, the migration status occasionally shows incorrect values. Occasionally while the Migration service is running, the migration status values for the total number of bytes being migrated and the total number of objects being migrated are incorrect. This occurs regardless of how many bytes or objects are actually migrated. Once the migration completes, the migration status values become accurate.

Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: https://knowledge.hitachivantara.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact