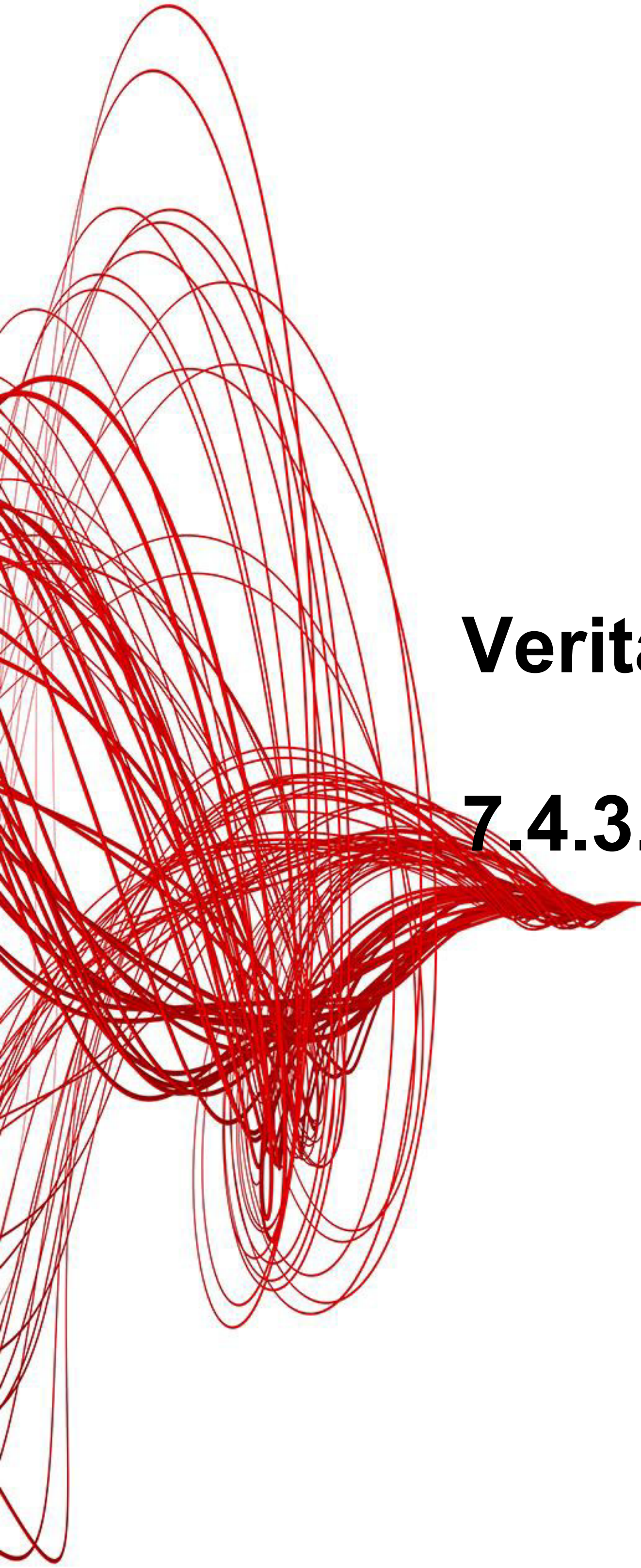

Veritas Access Appliance

7.4.3.300 Release Update

Linux

VERITAS™

The truth in information.

Contents

About the release

This release update includes critical product fixes and updated third-party packages that fix security vulnerabilities for the Veritas Access 3340 Appliance. Veritas recommends that you install this update to make sure that you have the latest product fixes. This patch can be installed on Veritas Access 3340 Appliance version 7.4.2.400, 7.4.3, 7.4.3.100, and 7.4.3.200. If you are on an earlier version of the product, upgrade to version 7.4.3, and then install the patch.

When you upgrade to Access Appliance version 7.4.3.300, Veritas Access software version 8.2.4.000, which supports Red Hat Enterprise Linux (RHEL) 7.9 is installed on the appliance.

For upgrading Veritas Access 3340 Appliance to 7.4.3.300, refer to the following technote:
https://www.veritas.com/support/en_US/article.100052815

Note: This document is an incremental update that describes the fixes in the 7.4.3.300 release update. For information about the enhancements and issues fixed in the previous releases, see the Access Appliance Release Notes version 7.4.3 on SORT (https://sort.veritas.com/documents/doc_details/AAPP/7.4.3/Veritas%203340/Documentation/).

Fixed issues and enhancements in this release

The following issues are fixed in the Access Appliance 7.4.3.300 release:

Critical security vulnerability fixes
OS Components:

CVE-2020-25704, CVE-2020-36322, CVE-2020-36385, CVE-2020-36518, CVE-2020-7598, CVE-2021-20271, CVE-2021-22060, CVE-2021-22096, CVE-2021-22118, CVE-2021-22543, CVE-2021-44906, CVE-2022-22950, CVE-2021-3653, CVE-2021-3656, CVE-2021-3712, CVE-2021-37576, CVE-2021-4034, CVE-2021-41617, CVE-2021-42739, CVE-2021-43527, CVE-2021-43527, CVE-2021-45417

Third-party components:

BDSA-2021-3401, CVE-2014-3643, CVE-2018-11087, CVE-2020-13936, CVE-2021-20330, CVE-2021-22569, CVE-2021-28168, CVE-2021-32036, CVE-2021-32718, CVE-2021-32719, CVE-2021-3765, CVE-2021-42340, CVE-2021-42550, CVE-2021-43859, CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, CVE-2021-45105, CVE-2022-0155, CVE-2022-0536, CVE-2022-21676, CVE-2022-23181

Fixed issues

- APPCPE-2970: StorageManagement.py --reset does not work when disks are shared.
- APPCPE-3435: **CIFS > localuser add** command fails when the CIFS server is started in CTDB clustering mode.
- APPCPE-3595: Unable to start the Access Appliance GUI in certain situations after upgrading from version 7.4.2.x.
- APPCPE-4188: Failed to reconfigure the deduplication server after upgrading from version 7.4.2.x.
- APPCPE-4243: The **Manage > Software > UpgradeStatus** command reports 1% completion status for more than 24 hours.
- APPCPE-4261: Failed to reset the storage after modifying disk configuration.
- APPCPE-4263: After bond creation, the second IP address is deleted from the cluster.
- APPCPE-4362: Fix critical security vulnerabilities present in Apache Log4j.
- APPCPE-4510: Cannot return to the system prompt on the host when password expires during a rolling upgrade.
- APPCPE-4900: The Access command **storage>disk list paths** does not display the multiple paths of the disks in a multi-path environment.
- APPCPE-5342: The **Support> Test Software** command does not validate the S3 Self Test even if it is configured.

- APPCPE-5480: Veritas Volume Replicator (VVR) replication enable hangs if SMTP is enabled.

Enhancements
The following enhancements are included in the 7.4.3.300 release:

- APPCPE-4158: Removal of stale RPMs after upgrading from Access Appliance version 7.4.2.400 to 7.4.3.300.
- APPCPE-4236: Added support for 16 GB Dual Inline Memory Module (DIMM).
- APPCPE-4237: Enhance hardware monitoring to detect the new Intel® X550-T2 10Gb NIC card on the appliance and monitor and report the card status.
- APPCPE-4731: Prevent user from restarting the node while upgrade is in progress.
- APPCPE-4734: Added the reboot status of each node during cluster upgrade.
- APPCPE-4789: Enhancements to the upgrade framework to make it more robust.
- APPCPE-4872: Preupgrade enhancements to verify MongoDB certificate.

Note: APPCPE numbers are for Veritas Support reference only.

Known issues

APPCPE-5183: Unable to roll back the system after an attempt to upgrade from 7.4.2.400 to 7.4.3.300 failed.
On 7.4.2.400, file system deduplication was enabled for some of the file systems. When file system deduplication is enabled, the **dedup_schedd_group** service group is created. However, when the file system deduplication is disabled, the group is not deleted. File system deduplication is no longer supported on 7.4.3.x. During the upgrade, the group could not be brought online, causing the upgrade and roll back to fail.
Workaround:
Delete the **dedup_schedd_group** service group before upgrading.

APPCPE-5347: Self test failed for storage_s3test
There is not enough free space in the storage pool to create an S3 bucket.
Workaround:
Ensure that the storage pool used by the object access server has sufficient free storage to create a bucket as per the size and type specified by the **fs_size** and **fs_type** parameters. The S3 self test is executed during an upgrade if the object access service is enabled, and the upgrade might fail if no bucket could be created.

APPCPE-5430: Upgrade may fail if operations such as OS reboot, cluster restart, and node stop and shutdown are used during the upgrade.
Performing any of the following operations during an upgrade can lead to an upgrade failure and the cluster might go in an inconsistent state. It is recommended that these operations should not be performed until the upgrade completes successfully.

- Logging into maintenance mode and executing OS commands such as reboot and shutdown.
- Logging into a node and executing commands such as cluster reboot, shutdown, and stop from the command-line interface.
- Executing node maintenance operations from the UI such as shutdown node and start node.
- Operations that will disrupt network connections such as unplugging the network cable.

Workaround:
There is no workaround for this issue.

APPCPE-5461: Upgrading from version 743.200 to 743.300 causes the replication continuous status *fs_name* command to hang.
Workaround:
Run the **systemctl restart vras-vradmind** command.

APPCPE-5595: Appliance upgrade from version 7.4.2.400 to 7.4.3.300 failed if the CTDB clustering mode is configured for a CIFS server.
A race condition might cause this issue.
Workaround:
Complete the following steps before you begin the upgrade:

1. Stop the CIFS server using the **CIFS> server stop** command.
2. Set security to user level using the **CIFS> set security user** command.
3. Start the CIFS server using the **CIFS> server start** command.
4. Stop the CIFS server using the **CIFS> server stop** command.

Complete the following steps after the upgrade:

1. Set the security to **ads** for the Active Directory Server domain controller using the Network> **ad set** command.
2. Enable Active Directory client to use Active Directory for authentication using the **Network>net ad**

enable command.

3. Start the CIFS server using the **CIFS> server start** command.

APPCPE-5640: Upgrade from version 7.4.2.x and 7.4.3.x to 7.4.3.300 fails during the preupgrade check (S3_selftest) if the management console and CVM master are not on same node of cluster.
Workaround:

1. Check on which node the ManagementConsole service group is online:
   ```
   #hagrp -state ManagementConsole
   #Group Attribute System Value
   ManagementConsole State node_01 |OFFLINE|
   ManagementConsole State node_02 |ONLINE|
   ```

2. Check on which node the CVM master is running:
   ```
   #/opt/VRTS/bin/vxclustadm nidmap
   Name CVM Nid CM Nid State
   node_01 1 0 Joined: Master
   node_02 0 1 Joined: Slave
   ```

3. If both the management console and the CVM master are not on the same node, set ManagementConsole node as Master using the following command:
   ```
   #/opt/VRTS/bin/vxclustadm setmaster <nodename>
   #/opt/VRTS/bin/vxclustadm nidmap
   Name                            CVM Nid     CM Nid      State
   node_01                         1           0           Joined: Slave
   node_02                         0           1           Joined: Master
   ```

4. Perform step 1 and step 2 to verify that the ManagementConsole and CVM master are on same node.

For information on all the other features, refer to the Access Appliance 7.4.3 documentation which is available online. The latest version of the product documentation is available on the SORT website.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at veritas.com or follow us on Twitter at @veritastechllc.

Veritas World Headquarters 2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com
For specific country offices
and contact numbers,
please visit our website.

The truth in information.