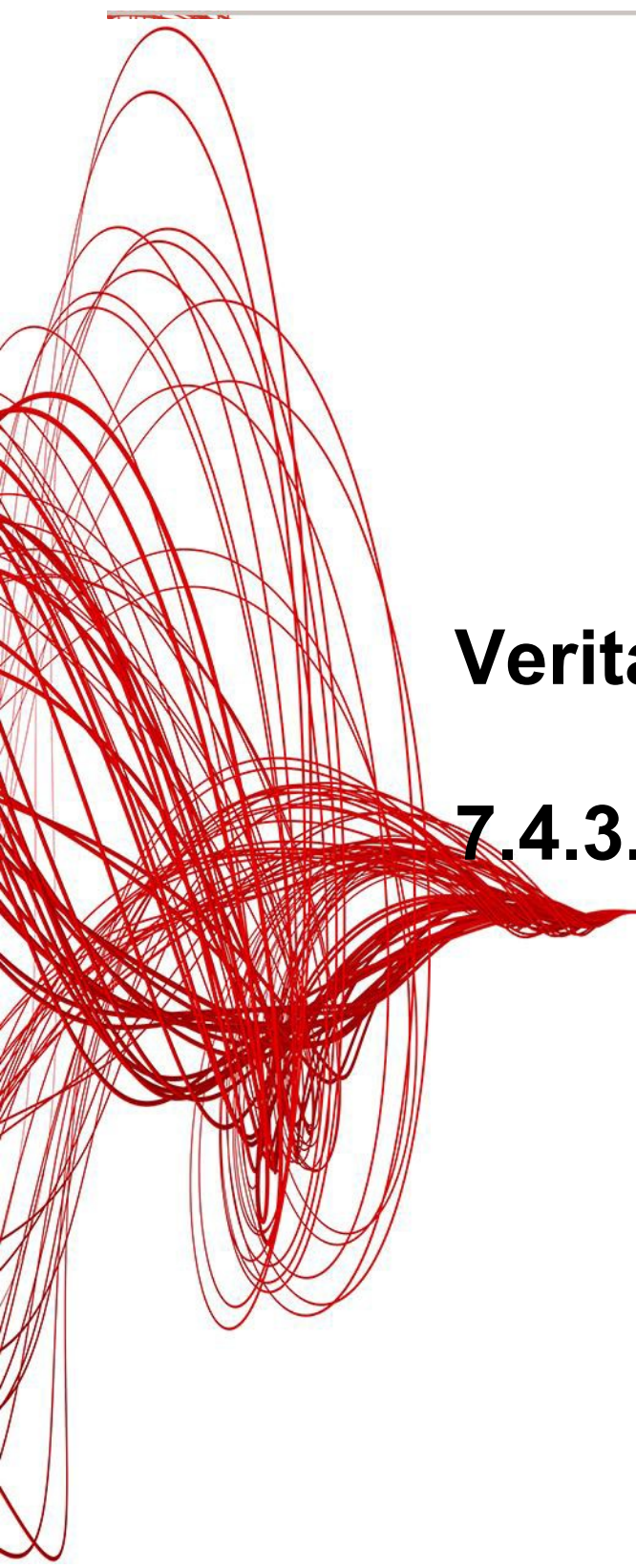

Veritas Access Appliance

7.4.3.200 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 7.4.3 release. 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, and 7.4.3.100. 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 7.4.3.200, Veritas Access software version 8.2.3.000, which supports Red Hat Enterprise Linux (RHEL) 7.9 is installed on the appliance.

For upgrading Veritas Access 3340 Appliance to 7.4.3.200, refer to the following technote:
https://www.veritas.com/support/en_US/article.100051842

Note: This document is an incremental update that describes the fixes in the 7.4.3.200 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 7.4.3.200 release:

Critical security vulnerability fixes
OS Components:

CVE-2016-4658, CVE-2020-27777, CVE-2021-3715, CVE-2021-22555, CVE-2021-23840, CVE-2021-23841, CVE-2021-29154, CVE-2021-29650, CVE-2021-30465, CVE-2021-31535, CVE-2021-32399

Third-party components:

CVE-2018-10237, CVE-2018-11087, CVE-2021-22116, CVE-2021-22117, CVE-2021-22119, CVE-2021-32718, CVE-2021-32719, CVE-2021-35515, CVE-2021-35516, CVE-2021-35517, CVE-2021-36090, CVE-2021-39139, CVE-2021-39140, CVE-2021-39141, CVE-2021-39144, CVE-2021-39145, CVE-2021-39146, CVE-2021-39147, CVE-2021-39148, CVE-2021-39149, CVE-2021-39150, CVE-2021-39151, CVE-2021-39152, CVE-2021-39153, CVE-2021-39154

Issues

- APPCPE-2490: Unable to configure AD server on IPv6 Access Appliance
- APPCPE-2956: Access upgrade from 7.4.2.x facing issue with SDCSS daemon using high memory
- APPCPE-2962: After upgrade to 7.4.3.200 ISCSI target creation command fails with unknown error
- APPCPE-2963: Storage command-line interface commands are getting hung during data upload from glacier to primary tier
- APPCPE-2988: Unplanned failover of episodic replication job is failing when bond over VLAN is configured between source and target
- APPCPE-2994: Replication continuous config auth command is successful even when virtual IP is not assigned for continuous replication service
- APPCPE-3010: Issues with dedupe reconfiguration with FIPS enabled
- APPCPE-3060: Shadow partition volume size non-adjustable during upgrade to 7.4.3.200
- APPCPE-3086: Cloud tiering configuration does not have interface name option
- APPCPE-3200: Upgrade failed because BIOS firmware test failed
- APPCPE-3209: Unable to log in to deleted node from cluster
- APPCPE-3230: Upgrade failed because of insufficient free space to back up MongoDB data
- APPCPE-3392: Unable to delete S3 bucket

- APPCPE-3485: Error info file not present in `debuginfo.tar` file for unconfigured module
- APPCPE-3757: Unable to see DIMMs in **Monitor > Hardware ShowHealth**

Enhancements

The following enhancements are included in the 7.4.3.200 release:

- APPCPE-3082: Introduced a new alert, which is displayed if the Veritas Data Deduplication (VDD) storage exceeds 90% instead of generating alerts for individual file systems created for VDD.
- APPCPE-3083: Introduced summary option in **debuginfo** command to collect the configuration summary for all modules. For example, **Support> debuginfo upload all file:///log/.LOGROOT/summary**
- APPCPE-3084: Improved compression techniques for generating log packages, which reduces the time to archive and upload the data to Veritas Support and saves storage space.
- APPCPE-3085: The **debuginfo** command now creates an archive of logs for each node, which helps to extract the logs of each node to separate directories, preventing accidental overwriting of the data.

Note: APPCPE numbers are for Veritas Support reference only.

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.