Avere OS 5.1.1.2 Release Notes
2019-01-07
Table of Contents

New in Avere OS 5.1.1.2 ......................................................................................................................... 1

Security updates ................................................................................................................................. 1
  SSL and TLS updates ......................................................................................................................... 1
  Permitted cipher suites ..................................................................................................................... 1
  Update private object storage to maintain compatibility ................................................................. 1
  SSH server updates ......................................................................................................................... 1

Resolved issues ................................................................................................................................... 3
  Cloud object store ........................................................................................................................... 3
  Filesystem ........................................................................................................................................ 4
  General ............................................................................................................................................ 5
  NFS ................................................................................................................................................ 6
  Security .......................................................................................................................................... 8
  SMB/CIFS ....................................................................................................................................... 8
  vFXT ............................................................................................................................................... 9

Contact Microsoft Customer Service and Support ............................................................................. 10

Copyright Information

Copyright © 2019 Microsoft Corporation. All rights reserved.
Specifications are subject to change without notice.

No part of this document covered by copyright may be reproduced in any form or by any means –
graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic
retrieval system – without prior written permission of the copyright owner.

The product described in this document may be protected by one or more U.S. patents, foreign patents,
or pending applications.
New in Avere OS 5.1.1.2

Avere OS 5.1 includes bug fixes, feature improvements, and significant security enhancements.

Security updates

This release improves security standards in several areas in order to comply with Microsoft security requirements.

Additional changes and bug fixes are documented in the Resolved issues - Security section later in this document.

SSL and TLS updates

Avere OS now requires the following standards for SSL and TLS:

- TLS1.2 must be enabled
- SSL V2 and V3 must be disabled

TLS1.0 and TLS1.1 may be used for backward compatibility with private object stores; contact Microsoft Customer Service and Support for details.

Permitted cipher suites

Microsoft security requirements permit the following TLS cipher suites to be negotiated:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

The cluster administrative HTTPS interface (used for the Avere Control Panel web GUI and administrative RPC connections) supports only the above cipher suites and TLS1.2. No other protocols or cipher suites are supported when connecting to the administrative interface.

Update private object storage to maintain compatibility

The SSL and TLS changes in this version can impact customers using private object storage cloud core filers that are not updated to the current standard.

If the encryption software on your private cloud core filer is incompatible with the above cipher suites and TLS 1.2, you might lose access to the core filer.
CAUTION
Your Avere cluster might lose connectivity to your private object store core filer after installing this update if the core filer does not use compatible encryption software. Contact Microsoft Customer Service and Support before installing Avere OS 5.1 to avoid possible service disruption.

For compatibility with this version of Avere OS, your private object store cloud core filer must meet these requirements:

- TLS 1.2 must be enabled
- SSL V2 and V3 must be disabled
- The TLS cipher suites in the permitted cypher suites list above must be supported

Consult your private object storage vendor to confirm that it complies with these standards. Take any additional necessary steps to ensure that the private object environment is correctly updated and configured.

If your core filer cannot be brought into compliance, there is a temporary workaround available through Microsoft Customer Service and Support. Remember to remove this workaround after your core filers have been updated.

In general, it is a good practice to update and audit your private object core filers to maintain security standards.

**SSH server updates**

To meet Microsoft security standards, the security of the cluster node SSH server has been tightened.

Remote login as the superuser “root” has been disabled. If remote SSH access is required under the guidance of Microsoft Customer Service and Support, you must log in as the SSH “admin” user, which has a restricted shell.

The following SSH cipher suites are available on the cluster SSH server. Make sure that any client that uses SSH to connect to the cluster has up-to-date software that meets these standards.

<table>
<thead>
<tr>
<th>Ciphers</th>
<th><a href="mailto:aes256-gcm@openssh.com">aes256-gcm@openssh.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="mailto:aes128-gcm@openssh.com">aes128-gcm@openssh.com</a></td>
</tr>
<tr>
<td></td>
<td>aes256-ctr</td>
</tr>
<tr>
<td></td>
<td>aes128-ctr</td>
</tr>
<tr>
<td>MACs</td>
<td><a href="mailto:hmac-sha2-512-etm@openssh.com">hmac-sha2-512-etm@openssh.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a></td>
</tr>
<tr>
<td></td>
<td>hmac-sha2-512</td>
</tr>
<tr>
<td></td>
<td>hmac-sha2-256</td>
</tr>
<tr>
<td>KEX Algorithms</td>
<td>ecdh-sha2-nistp521</td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp384</td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp256</td>
</tr>
<tr>
<td></td>
<td>diffie-hellman-group-exchange-sha256</td>
</tr>
</tbody>
</table>
Resolved issues

Cloud object store

23802  Improved management of the cloud snapshot database to avoid system panics. Before this change, the snapshot database object could grow very large, even though the number of actively needed snapshots was small. This fix improves database parsing efficiency and also ensures that the snapshot object file is not larger than the number of undeleted snapshots.

25227  Fixed an incorrect alert that suggested a cloud bucket or container could not be found after an Avere OS upgrade.

25717  Reduced the number of log entries from the certificate verifier component.

25837  Added automation to some cloud core filer modifications so that they no longer require service restarts.

25845  Fixed a bug in a database that could inappropriately stop the process that writes data to the cache disks.

25913  Improved performance of file creates and file lookups in directories by adding bloom filter support.

25992  Changed the way Avere OS handles a REST parse error for non-data objects from AWS storage. Now it returns a jukebox code instead of returning I/O error.

25995  Fixed a problem with snapshot identifiers to ensure that only the latest snapshot ID is used.

26157  Implemented a timer to fix timeout issues with HA barriers.

26159  Added a timer to reduce TCP connections on overwhelmed Amplidata core filers.

26179  Reduced memory consumption by improving memory management in the cloud module memory system.

26187  Fixed two issues related to certificate checking.

26235  Fixed a problem that could sometimes cause a system restart because flags were set incorrectly during express snapshot creation.

26338  Eliminated an issue that could cause a system restart when reattaching cloud storage to a cluster with a newer Avere OS version than used previously.

26341  Fixed an issue where a restart would occur if an object handle snapshot did not exist in the cloud core filer.

26366  Fixed a logic error that could cause a loop because a variable was defined in the wrong location.

26401  Removed string buffer bugs found under boundary conditions.

26469  Fixed an issue that could cause directory segments to become inaccessible after an upgrade, blocking accesses to multiple entries in the directory.
Addressed an issue where cloud object segment sizes and number of segments were improperly set, causing a service restart.

Disabled a bloom filter to fix a problem where a move from a source to a destination would cause a core loop if the destination already had the file.

**Filesystem**

- **23719**: Added a feature to enable asynchronous writes and improve small file write performance.
- **23849**: Fixed an issue that could cause continuous restarts in the migration code.
- **24307**: Improved performance of rename actions by 30%.
- **24506**: Resolved a problem that affected read-ahead caching on the Avere cluster. Linux-based NFS clients maintain their own client-side file caches, and this cache is populated with the client’s own read-ahead. If the file being read is not in the Avere cache, and the NFS client read-ahead calls arrive out of order (that is, the read for the file’s offset-zero segment comes in later than other reads), the Avere read-ahead calls for cache population of a "cold" file were not being sent.
- **24562**: Added a feature to automatically identify and remove orphaned inodes.
- **24721**: Added a custom setting to adjust the threshold that triggers local file replicas to be created.
- **24791**: Added tracking for HA operations.
- **25003**: Fixed a race condition in detecting the available space for internal metadata structures.
- **25084**: Added code to fix a race condition in the token request system that could happen when failover caused changes in a mirror relationship.
- **25376**: Fixed resource leaks in the cloud filesystem that caused occasional crashes due to memory shortages.
- **25439**: Added more visibility into the status of the HA voter component.
- **25949**: Improved token management when recycling files from the cache.
- **25963**: Fixed an issue that could cause a service restart when adding or removing nodes or upgrading software.
- **25970**: Corrected an incorrectly set flag that could cause long lookup times, timeouts, or system restarts.
- **25980**: Fixed a filesystem service restart caused by performing read-ahead operations on a file that was concurrently being reclaimed from the cache due to space constraints.
- **26040**: Changed code to correctly initialize the field _aclFlags.
- **26044**: Fixed an error updating a task counter. This issue could cause a system restart when the task was cleaned up.
- **26140**: Fixed an issue where temporary files prevented a migration job from completing.
Corrected a situation where token management references were lost, causing system restarts.

Updated code to also forward fsstat, pathconf, and fsinfo operations when always-forward is set.

Changed code to prevent unnecessary token revokes because the token owner was incorrectly identified.

Fixed a crash related to a race condition in the Avere Directory Name Cache component when recycling large numbers of files from the cache.

Accelerated performance of the version database.

Changed filesystem code to allow the Avere system to read a core filer directory even when some directory entries are inaccessible because of permissions. This change allows some core filer exports to be visible to the cluster and others to be ignored.

Fixed an issue where retrying certain operations eight times caused a restart.

Fixed code to prevent a filesystem restart caused by incorrectly cleaning up lock-related flags from failed operations.

Removed a division-by-zero error bug that could be triggered by an inode file size of zero.

Fixed a bug where an ENOENT error could cause the node to lose connection to a junction.

Updated code for directory entry pruning to avoid problems caused by long queues.

Fixed an issue that unnecessarilly incremented an iterator on a data structure that was being erased.

Changed log procedures to avoid repeated messages if HA is not enabled.

Updated the help file for the XML-RPC method alert.override() to remove the incorrect implication that alert UUIDs are deprecated.

Added time stamps and time ranges to traces and XML-RPC output.

Fixed a filehandle leak in the Avere OS maintenance process.

Added performance metrics to logs and XML-RPC output.

Fixed a display issue in the Avere Control Panel related to directory service polling updates.

Updated the API error message for proper formatting of private keys.

Fixed an issue that caused the Avere OS management web service to restart.

The Avere Control Panel now shows which cluster node is primary and which node the session is connected to. This information appears at the right side of the cluster name.
Output about cluster upgrade status now displays plain text instead of HTML-encoded text.

Updated the hidden alerts function to consistently apply parameter filters.

Added a **Users** table to the dashboard that displays the IDs of recently active users and the number of operations they’ve performed. User activity can be displayed by node or cluster-wide (all nodes).

Adjusted permissions for read-only XML-RPC API users to make sure that they can access non-modifying methods.

Improved the layout and usability of the Alerts table in the Avere Control Panel dashboard.

Fixed a bug that prevented support uploads from including custom settings.

Fixed a bug in lock contention handling when reading the configuration database.

Custom graphs in the **Analytics** tab now display core filer names in the legend instead of internal names.

Fixed an issue caused by locks allocating more memory than needed.

Fixed a bug that prevented uploading a new software image from a local machine.

IP addresses on the IPMI settings page are now links that open a connection to that IPMI port.

Fixed a software alert message to correctly identify software upgrade status.

Upgraded to FreeBSD 11.2.

Corrected an issue where a memory-related default was not set correctly on FXT 5850 hardware systems.

Improved security by removing the ability to reuse cookies to execute XML-RPC commands.

Fixed an issue where the SPS agent would stop and not restart.

Added a file locking option in the cache policy management section of the Avere Control Panel. Use the **Advanced** settings section to select or clear the **Enable NLM caching** checkbox.

Added a filtering option in the **Alerts** table of the Avere Control Panel Dashboard. You can choose to view only conditions, only alerts, or both conditions and alerts.

**Migration**

Fixed an issue where a migration would not release an inode at file close unless it was a destroy operation.

Fixed an issue that caused migration code to restart continuously.

Changed code to properly repopulate a migrated subdirectory in the file system. This change prevents getting a stale junction after a junction refresh following a data migration.
25708 Fixed code to correctly handle cloud snapshot deletion when a snapshot has already been deleted from some nodes.

26140 Fixed a problem where some tasks were not marked as complete after a migration.

NFS

10363 Fixed several defects involving NFS export policy reference counts. These issues could result in the inability to delete an unused policy. Upon upgrade, this change corrects NFS export policy reference counts that were set incorrectly because of these defects.

14237 This ticket increases the number of supported NLM clients per vservers client-facing address from 4096 to 10000. This increased limit is consistent with the 10000 NFS client limit per node when only one client-facing address per node is allocated. This change only applies to new vservers created with a build containing this change. Downgrades to builds not containing this change are prohibited if the new feature has been used, because the new vservers will not process lock operations correctly after downgrade.

19883 Addressed NIST security vulnerability CVE-1999-1225.

24876 Improved LDAP/AD compatibility of the Avere Control Panel login system. Specifically:
  • Removed the requirement to enable both LDAPS and LDAP with StartTLS on the LDAP server. Now, only LDAPS is required. (Enabling LDAP with StartTLS is optional.)
  • Allows custom LDAP and LDAPS ports to be configured. Use the XML-RPC method dirServices.modify login to set the variables LDAPport or LDAPSport.
  • Attribute queries can now be set to ad or rfc2307 instead of the default, auto. The auto setting searches for both types of attributes, which is slower and can cause timeouts when used with large LDAP trees. Use the XML-RPC method dirServices.modify login to set the variable loginQueryAttributes.

25023 Addressed an internal configuration timing race that could cause the filesystem service to fail during startup after a software upgrade.

25491 Improved the NFS core filer RRDNS change procedure.

25546 Implemented NLM lock caching for NAS core filers. This feature is available only on new clusters created with a build containing this change. NLM lock caching for NAS core filers is enabled by default for system cache policies that do not allow directly connected clients. Custom cache policies can control the behavior using the XML-RPC methods cachePolicy.create() and cachePolicy.modify() by specifying the enableNlmCaching parameter.

25978 This change fixes a defect where the XML-RPC method nfs.modify() did not correctly handle changes to a subset of the available options. The workaround for this defect is to specify all of the options in each call to nfs.modify().
Added a buffer size check to prevent a possible internal string overflow.

Fixed two defects found in an on-box debugging tool. These failures are not thought to have caused any problems at customer sites.

Security

The procedure for storing cluster login information used with the Cluster Manager feature has changed. The Cluster Manager allows you to monitor multiple clusters from a single web page.

Before this change, the usernames and passwords used to access the remote clusters were stored in cleartext in an internal configuration file. The configuration file could be uploaded to the Avere support portal as part of troubleshooting, possibly exposing the passwords outside the cluster.

Now the login information is stored in a protected key distribution database that is stored on the cluster and never uploaded for support.

It is strongly recommended that all affected customers change the administrative passwords on clusters monitored in the Cluster Manager. Configure the Cluster Manager to use read-only accounts to connect to the remote clusters.

Improved security by denying root access over SSH except from addresses in the local cluster.

Updated PHP software to version 5.6.37.

Fixed port vulnerabilities identified by the following NIST CVE numbers:

- CVE-2017-15710
- CVE-2017-15715
- CVE-2017-3738
- CVE-2018-0495
- CVE-2018-0732
- CVE-2018-0737
- CVE-2018-1283
- CVE-2018-1301

When an HTTP request is redirected to HTTPS, the system now returns the status code 308 (moved permanently) instead of 302 (moved temporarily).

SMB/CIFS

Addressed a defect that could result in a CIFS service restart if the user token was unknown.

Added interlocks that prevent advanced SMB/CIFS share options associated with POSIX mode bit junctions from being set on CIFS ACL junctions.

Fixed an issue that prevented users with non-read access to a file or directory from accessing the file or directory at all.
23716 Addressed a problem that affected NetApp Clustered Data ONTAP core filers and prevented adding or modifying a subdirectory junction when the export policy prevented one of the components of the filepath from being created.

23843 Addressed a defect in Data Management out-of-sync processing for CIFS ACL migrations to cloud core filers. Out-of-sync processing of Native Identity File/Directory creations now fetches the source ACL from an internal cache rather than failing to fetch from the core filer.

23895 Resolved an issue where client calls to fetch SMB ACLs could cause recursive forwarding between FXT nodes due to an internal file-operation-routing loop.

25154 Addressed a defect in the receipt of Kerberized NFS client operations that could cause a filesystem service restart.

25576 Corrected an error that prevented the Force directory mode setting from displaying in the CIFS share details page on the Avere Control Panel.

25866 Fixed an issue where an SMB1 client could cause a CIFS service restart by performing repeated authentications.

25872 Updated code to prevent a filesystem service restart that could occur when invalid UTF-8 characters were present in NFS directory entry names. Problems were seen when these invalid directory entries were reported in the Data Management or Hot Files features.

26190 Fixed a problem that could cause a filesystem service restart when an SMB client lists large directories through a CIFS ACL junction.

26462 Addressed a defect that could occur when a NAS core filer returned an error in response to an SMB1/SMB2 FILE_INFO query operation. This defect caused failures with two different symptoms:
  • A long running operation on an SMB/CIFS client, which could possibly result in an operation timeout.
  • An eventual restart of the CIFS ACL service because of a memory leak related to the original core filer error response.

26506 A problem was fixed that caused an NFS username lookup to sometimes return the UID of a different user that had the same primary GID. This could cause SMB clients to see incorrect file ownership or incorrect ACE identities in access control lists.

26522 For increased security, new vservers are now configured with outbound NTLMSSPN disabled. Contact Microsoft Customer Service and Support for more information about the implications of this change.

vFXT

24457 Updated vFXT deployment code to ensure that AWS tags are consistently applied.

24700 Removed external internet dependencies from vFXT systems running in AWS C2S.

26592 Fixed an issue that caused a service restart when attempting to look up network configuration in GCE projects with large numbers of virtual machines.
26595  Fixed an issue that could cause VM instance lookup to fail if the region information
        returned by the GCE API did not include zones for each region.

**Contact Microsoft Customer Service and Support**

Microsoft Customer Service and Support can be reached by website, phone, or email.

**By web:**  http://www.averesystems.com/support

**By phone:**  1-888-88-AVERE, Option 2 (Toll-Free)
               1-412-894-2570, Option 2

**By email:**  averesupport@microsoft.com