Actifio Global Manager (AGM) 10.0.5 Release Notes

Copyright, Trademarks, and other Legal Matter

February 14, 2023

Contents

1 Introduction

This document includes the release notes for Actifio Global Manager (AGM) 10.0 and its follow-on service packs.

The latest version of the Actifio Global Manager (AGM) Release Notes can be found on the ActifioNOW Customer portal.

It includes the following topics:

Upgrade Paths to AGM 10.0.5

AGM running on 10.0.2 or higher can be upgraded directly to 10.0.5.

AGM running versions older than 10.0.2 must be upgraded to 10.0.2 first, and then upgrade to 10.0.5. Refer to the release notes for 10.0.2 for details on the supported upgrade paths to that releases.

If catalog is configured on the AGM, then the upgrade path will include a significant upgrade to the catalog database. This requires additional steps.

- AGM must be upgraded to 10.0.4, and then apply the latest AGM October Monthly Hotfix Rollup (MHR) or higher.
- Customer Success must perform some configuration changes, followed by a reboot of the AGM prior to upgrading to SP5.

> ***Note:*** *This update may result in some down time for the catalog after being installed, while the rest of AGM is functioning normally. The duration will depend on the size of the cataloged data, and could be as long as 24-48 hours in the worst case. Wait for catalog jobs to begin succeeding again before continuing.*

- Perform the upgrade to 10.0 SP5.

Note: *This update may result in some down time for the catalog after being installed, while the rest of AGM is functioning normally. The duration will depend on the size of the cataloged data, and could be as long as 24-48 hours in the worst case. Wait for catalog jobs to begin succeeding again before continuing.*

Product Documentation

The following table summarizes the various documents in the AGM documentation library.

Document	Description
Installing and Upgrading Actifio Global Manager on VMware Server	Provides information on how to deploy and install the AGM OVA file using the VMware vSphere Web Client.
Installing and Upgrading Actifio Global Manager on Hyper-V Server	Provides information on how to deploy and install the AGM OVA file using the Hyper-V Server.
Deploying Actifio Global Manager in AWS	Provides information on how to deploy AGM in AWS.
Deploying Actifio Global Manager in Microsoft® Azure Cloud	Provides information on how to deploy AGM in the Azure cloud.
Deploying Actifio Global Manager in a Google Cloud Platform	Provides information on how to deploy AGM in the Google Cloud Platform.
Actifio Global Manager Release Notes	Contains a summary of new features and functionality, installation notes, and known limitations and restrictions with each AGM release.

Product documentation for AGM is provided through an Online Help system that is integrated directly into AGM and accessed from AGM. The Help provides step-by-step instructions on how to use the Dashboard, Domain Manager, SLA Architect, Application Manager, Catalog, System Monitor, Report Manager, and Upgrade services in AGM. We also provide field-level help. The field-level popup also provides a AGM context-sensitive link to the relevant topic in the Help.

The ActifioNOW Customer Portal

You can always find the latest documentation for AGM and Actifio CDS or Sky appliance releases on the ActifioNOW customer portal. This includes the latest version of the Actifio Global Manager (AGM) Release Notes, which may be more current than what is included as part of the AGM Documentation Library. You can also find a set of Service Pack Read Me documents for this AGM release.

During the configuration and initialization of your Actifio appliance your Actifio representative provides you a username and password for the ActifioNOW customer portal.

From the customer portal, you can obtain detailed reports about your Actifio appliance, as well as search the portal's knowledge base for answers to specific questions. ActifioNOW is your singular portal for Actifio product information, certified knowledge, the latest best practices, immediate help, and extensive learning resources.

To log into the ActifioNOW customer portal:

1. Go to: https://now.actifio.com.
2. When prompted, enter the user name and password provided by your Actifio representative.
3. From the ActifioNOW customer portal, you can access:
   - **Product Documentation** - View the user documentation for your Actifio products and releases.

     https://actifio.force.com/c2/apex/C2ProductInformation
   - **Knowledge Base** - Search across all of the available content for relevant articles.

     https://actifio.force.com/c2/apex/C2ProductInformation

Actifio Support and Service

Access these locations for help with your Actifio product suite:

Customer Support Phone	**From anywhere**: +1.315.261.7501 **US Toll Free**: +1.855.392.6810 **Australia**: 0011 80016165656 **Germany**: 00 80016165656 **New Zealand**: 00 80016165656 **UK**: 0 8000155019
Customer Support Email	support@actifio.com
Customer Support Portal	http://support.actifio.com/

2 AGM 10.0 SP5 Enhancements and Resolved Issues

This chapter describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 10.0 SP5 release.

This chapter includes the following topics:

For a comprehensive list of known defects in AGM 10.x, see Known Defects on page 45. For a list of CVE fixes, see Security and Vulnerability Issues on page 53.

New Features and Functionality in AGM 10.0 SP5

The following are the new features, enhancements, and changes in AGM 10.0 SP5 release:

Database Enhancements

Highlights:

- MongoDB support for sharded clusters
- Parallel DB and Log backups
- Enhanced retention/expiration management for database logs, added the ability to hold database logs relevant to a database backup for as long as the backup is retained. Configuration is performed through the expiration management feature.
- Ability to provision extra storage for use in a mount of an Oracle database.

Benefits:

- Ability to protect and recover MongoDB sharded clusters
- Database log backups do not need to wait for database backups to complete, which results in an improved ability to meet the specified RPO.
- Point in time recoveries are now possible, even beyond the normal log retention period, when the database backup retention has been updated to indicate logs should be saved.
- Oracle database mounts used for test data management will no longer need to consume disk space on the Oracle server if extra space is needed, it can be provisioned as part of the mount operation

Disaster Recovery Enhancements

Highlights:

- All new conversion engine for VMware to GCE recoveries

Benefits:

- Recoveries are faster and more consistent
- The support/compatibility matrix for operating systems is broader, with a faster ability to add new support when needed

Security Enhancements

Highlights:

- New right to independently manage users authorized to prematurely expire backups

Benefits:

- Provides additional flexibility for separation of administrative roles
- Reduces risk of a rogue employee prematurely expiring backups that have not been flagged for “enforced retention”.

Report Manager Enhancements

Highlights:

- Stand-alone Report Manager (RM) is no longer supported beginning with 10.0.5. Report Manager will only be supported when running in the AGM+RM configuration going forward.
- Customer Success can help to merge your stand-alone RM into an AGM, while maintaining all historical data.

Benefits:

- RM will benefit from a centralized security model, integrated with AGM instead of a single appliance.
- Fewer virtual machines need to be run as part of the Actifio solution
- Simpler upgrade process going forward

Deprecated Features

With the new conversion engine for VMware to Google Cloud Compute Engine (GCE) come the following reductions in features:

- Conversions of VMs into AWS and Azure are no longer supported
- Conversions are exclusively supported from VMware VMs
- Conversions from connector backups (systemstate applications) are no longer supported, including conversions from physical servers into VMware.

Resolved Issues in AGM 10.0 SP5

The following list summarizes the resolved issue in AGM 10.0 SP5:

Resolved Issues

Issue	Fix	Tracking
AGM		
[Enhancement]: GCE onboarding wizard is enhanced to display all the project IDs from the **Project ID** drop-down.		203782563
Unable to mount the remote Dedup image to a target host when the primary Sky appliance is down.	This issue is now fixed.	208836421
[Enhancement]: Added a new API to do incremental add/remove for logical groups member management in Onboarding Wizard instead of complete replacement approach.		198328687
Enhancement: LDAP authentication is enhanced with Lookup Current Password field to update the defined configuration.		197292271 210602454
Unable to change the transport mode options from NFS to SAN while editing a vCenter host.	This issue is now fixed.	194680004
While performing cross project recoveries, the credentials drop-down displays all the valid and invalid credentials in the same list.	This issue is fixed and the credentials drop-down now displays valid and invalid credentials in two separate groups.	194863210
Enhancement: The OnVault pools in Appliance Configuration > Storage pools are enhanced to display Cloud - Google Cloud Storage as a default pool type.		191373784
Application onboarding shows incorrect status even though the application is already discovered.	This issue is now fixed.	229104150
Unable to perform the system recovery (RecoverSystem) if the AGM domain name contains Actifio.	This issue is now fixed.	212780959
Enhancement: For any App type, the friendly path of the target hosts of virtual machines is appended to the hostname with parenthesis ex: hostname (friendlypath).		228586352
AGM GUI allows to delete all the templates in the policy without any error message or warning.	This issue is now fixed.	228916450
AGM does not display Performance & Consumption Options when mounting the OnVault image. This issue is observed only for CDX-VX applications.	This issue is now fixed.	227709108

Resolved Issues

Issue	Fix	Tracking
Unable to allocate roles/org to LDAP users from AGM UI at user level with no LDAP group mapping.	This issue is now fixed.	226103827
The RMAN rate parameter in Application Details & Settings page accepts invalid range of values through AGM.	This issue is now fixed.	221407238
Sometimes, AGM creates multiple duplicate session timeout dialogs that consume significant memory.	This issue is now fixed.	214663820
Enhancement: The DB+log option is enhanced to show only for appliances running on 10.0.4 version or lower.		191769852
The “Apply SLA” dialog fails to display for catalog enabled applications when required fields are not specified.	This issue is now fixed.	211013240
Unable to upgrade AGM to 10.0.4 version due to the free disk space.		197135288
Appliances fail to show the connection status and reports as stale.		237988649
Enhancement: Added a new option “Copy HBD User Store Key to Target Host” to restore SAP HANA cluster.		190193717
After upgrading from 10.0.2 to 10.0.4, GUI contents are wiped out and RPM Package Manager (RPM) does not update.		211109549
For Remote Direct and LiveClone workflows, the Database options are missing in the Edit and RunNow screens for SQL and Oracle apps.	This issue is now fixed.	191994852
Sometimes AGM misses a backup entry in the list of backup images.	This issue is now fixed and It no longer misses the backup entries.	221909282
Added a warning message, if SLA is updated and the App has one or more preserved images.	This issue is now fixed.	219004166
Reporting		
In Report Manager 10.0.2, when generating a report of all the SQL clusters and hosts, the clustermemberdatatbl table is shown as empty.		195788684
Report Manager upgrade from 10.0.2 to 10.0.4 failed when /act/pgdata mounted on a different disk.		194060201

Resolved Issues

Issue	Fix	Tracking
Enhancement: Report Manager is enhanced to show GCP Instance when you apply the Application Type filter.		223056707
Scheduled real-time reports do not see email configuration changes until Report Manager service is restarted.		230365323
Fixed the issue that prevents updates to the pre-packaged set of reports in Report Manager 10.0.4.		227132786

3 AGM 10.0 SP4 Enhancements and Resolved Issues

This chapter describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 10.0 SP4 release.

This chapter includes the following topics:

- New Features and Functionality in AGM 10.0 SP4 on page 11
- Resolved Issues in AGM 10.0 SP4 on page 12

For a comprehensive list of known defects in AGM 10.x, see Known Defects on page 45. For a list of CVE fixes, see Security and Vulnerability Issues on page 53.

New Features and Functionality in AGM 10.0 SP4

The following are the new features, enhancements, and changes in AGM 10.0 SP4 release:

Enhancements to the Reporting Component

The following are the list of new features and enhancements added in this release:

SQL Server and SAP HANA Onboarding Wizard

Highlights:

- New Onboarding wizards for a focused and efficient onboarding process
- Allows single step discovery and protection for SQL Server Instances and Availability Groups, and SAP HANA databases.

Benefits:

- Fewer steps for users to onboarding SQL Servers.
- More intuitive user experience.

Enhanced Resiliency Director Support for Databases

Highlights:

- Added support for orchestrated recovery of additional databases, including Db2, MariaDB, MaxDB, MySQL, Oracle (both file system format and ASM), PostgreSQL, SAP HANA, SAP ASE, SAP IQ.
- Enhanced the SQL Server integration to support the ability to specify individual database names instead of only prefixes and suffixes.

Benefits:

- Scripting is no longer required for orchestrated recovery of database servers for any of the database engines supported by Actifio.
- Reduced RTO for DR recoveries of database servers.
- Greater reliability and repeatability for DR recoveries of database servers.

Deprecated Platforms in 10.0 SP4

- No currently supported platforms have support deprecated in 10.0 SP4.

Deprecated Platforms planned for the future

- Internet Explorer 11 will no longer be a supported browser with Actifio products beginning with 10.0 SP5.
- vCenter 5.5 and 6.0.x will be deprecated beginning with 10.0 SP5.
- Oracle 11g will no longer be supported effective October 31, 2021.
- CentOS 6.x will no longer be supported effective October 31, 2021.

Upgrade Paths

Actifio CDS and Sky systems running 8.x or 9.x can be upgraded to 10.0 SP4. Older versions need to be upgraded first to one of these releases.

- Actifio CDS systems running versions prior to 8.1.3 will require double-hop through 8.1.5 (then to 10.0 SP4).
- Actifio Sky systems running versions 8.1.1 & 8.1.2 will require the latest HF to avoid a double-hop through 8.1.5.
- Actifio Sky systems running versions prior to 8.1.1 will require double-hop through 8.1.5 (then to 10.0 SP4).

Actifio CDS firmware upgrade to 7.8 is required with 10.0 and is supported on CDS generations 4.0 and above. The older 7.3 and 7.5 firmware versions are not supported with 10.0 SP4.

Actifio CDX systems running 8.1.2 version first need to be upgraded to CDX 8.1.2.973 version (or above) before upgrading to 10.0 SP4.

Actifio CDX systems running 10.0.0 version need to apply HF 2323 before upgrading to 10.0 SP4.

Resolved Issues in AGM 10.0 SP4

The following list summarizes the resolved issue in AGM 10.0 SP4:

Resolved Issues

Issue	Fix	Tracking
AGM		
[Workflow] New application refresh fails with the error "JSONObject["key"] not found.	This issue is now fixed.	91702
The search box in the Applications field of App Manager allows to run JavaScript to access session cookies or perform other malicious actions.	This issue is now fixed by encoding the HTML entities to prevent switching into any execution content.	90770

Resolved Issues

Issue	Fix	Tracking
When a host is added in the AGM, and the hostname contains JavaScript code or malicious script, it is executed in the host grid.	This issue is now fixed.	90799
Non-admin users cannot disable the SLA if the application is protected or SLA is enabled by the admin user.	This issue is now fixed.	90624
The database and its backup image entries sometimes disappear in AGM GUI due to a UI issue.	This issue is now fixed by changing the configuration to delete appliances in two steps.	88179
An issue occurs while discovering the hosts if the hostname contains special characters.	This issue is now fixed by allowing the a-z, A-Z, 0-9 characters along with hyphen(-) and dot(.) for the hostname.	91002
Enhancement: Added support for project ID during ‘lscloudvm’, ‘addvm (VM discovery)’, and project ID validation during create/update credentials (testcredential, mkcloudcredential, chcloudcredential).		90828 90413
All entries are selected when the global check box is enabled on Add Application page.	This issue is now fixed by making changes to the pagination control.	91362
The Timeline Ramp view in the Application page is incorrect for some images protected with LogSmart policy and appearing in the Dedup and remote Dedup lanes.	This issue is now fixed.	91333
Enhancement: Log purge support in hours is extended for the DB2 database.		88963
LDAP implementation using ‘fast bind’ control (OID 1.2.840.113556.1.4.1781) is not supported by the Oracle Unified Directory LDAP server.	This issue occurs in a rare scenario. The ‘fast bind’ control support may not be required for LDAP implementation.	89673
The response of VM discovery in AGM takes a longer time.	This issue is now fixed.	89734
Deleting an application from AGM may sometimes delete all its backup entries.	This issue is now fixed by not using the call super.deleteObject().	90051
Enhancement: Added a new query parameter "show_all_paired_appliances" to get the complete list of paired appliances for a selected source appliance.		91205
'Target Appliance' drop down on Add Applications page shows only 11 Appliances even though the AGM has more than 11 appliances added to it.	This issue is now fixed by removing the cluster list limit.	91235
Enhancement: Added new functionality to restore multiple VMDKs into multiple data stores.		85466

Resolved Issues

Issue	Fix	Tracking
Enhancement: Cloud type name is now changed from ‘AZ’ to ‘Azure’.		75151
Enhancement: The orchestrator now sends the recovery time while performing a mount-and-migrate operation back to the same host.		72049
An SQL error occurs while updating ApplicationMomData if properties contain a quote.	This issue is now fixed.	88995
Enhancement: Added an option to turn On/Off ‘forcedirectio’ for both snapshots and mounts.		89034
Unmount Jobs for an application are not visible for a non-admin user if organizations are assigned to a host.	This issue is now fixed.	89635
Azure AD SAML IdP Metadata parsing issue occurs on optional attributes Signature RSAKeyValue Modulus & Signature RSAKeyValue Exponent.	This issue is now fixed by changing the optional attributes as not mandatory in IdP Metadata.	89485
Null pointer exception without stack trace details in the log history when the replication change request API call fails.	This issue is now fixed.	90100
The hostname is not persistent after upgrading the Actifio Global Manager from version 9.0.x to version 10.0.x.	Perform the below procedure and then upgrade from version 9.0.x to version 10.0.x. Perform actnet config hostname $(hostname) before running c7iso update to persist the old dhcp hostname.	89264
OnVault job expiration fails with the error “Cannot expire OnVault object while it's being mounted without using force option.”	This issue is now fixed.	91843
Azure AD SAML IdP Authnrequest issue occurs when the default implementation of authentication request for RequestedAuthnContext's comparison attribute is minimum, whereas Azure AD is expecting as an exact attribute.	This issue is now fixed by removing the AuthenticationContext policy from SAML authentication request.	89488
Reporting		
The Resource Consumption by Application report does not include unprotected applications.	This issue is now fixed by making the required changes to include unprotected application information.	89187
Schedules are not working after upgrade if it has RM long FQDN name.	This issue is now fixed by changing the column length to VARCHAR.	91396

Resolved Issues

Issue	Fix	Tracking
All the existing custom reports and schedules are deleted while upgrading from 10.0.1 to 10.0.2.	This issue is now fixed by updating the password fields to VARCHAR and removing the character limits.	90047
PostgreSQL shuts down while creating an index on the audit table.	This issue is now fixed by addressing the index-level memory issues.	90011

4 AGM 10.0 SP2 Enhancements and Resolved Issues

This chapter describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 10.0 SP2 release.

This chapter includes the following topics:

- New Features and Functionality in AGM 10.0 SP2 on page 17
- Resolved Issues in AGM 10.0 SP2 on page 19

For a comprehensive list of known defects in AGM 10.x, see Known Defects on page 45. For a list of CVE fixes, see Security and Vulnerability Issues on page 53.

New Features and Functionality in AGM 10.0 SP2

The following are the new features, enhancements, and changes in AGM 10.0 SP2 release:

Streamlined support for PostgreSQL

Highlights

- Actifio enhanced its out-of-the-box support for PostgreSQL. Databases are discovered automatically, transaction logs are managed as part of the SLA associated with the databases, and recovery to any point in time and creation of virtual clones are done entirely from the UI, either on-demand or as part of automated workflows.

Benefits

- Faster deployment and operational simplicity.
- Automated discovery, backup/capture, and recovery of all these databases.
- Log roll forward option to recover databases to any point in time.
- Automated deployment of virtual clones (application aware mount) for TDM use cases.
- No need for using customized scripts - support is out-of-the-box.

Expanded support of External Snapshot Pools with all databases

Highlights

- Customers can now use External Snapshot Pools (ESP) with all supported databases, in addition to Oracle and SQL Server, which were already supported. Customers can leverage their storage arrays' performance, connectivity, and availability by using the array native snapshots for Actifio's snapshot pool.

- Supported databases include Db2 (on Linux and AIX), SAP HANA, ASE, IQ and MaxDB, MySQL, MariaDB, and PostgreSQL.

Benefits

- Better performance on mounted images. Activity on virtual clones does not go through the Actifio appliance but rather directly between the host and storage array. This is especially important in test/dev environments.
- Better performance and RTO for DR when using external snapshot pools on the DR side. Data is updated and available in its intended target storage, so there is no need to copy it elsewhere.
- Better performance on database backups (data moves directly from array to array, without going through an Actifio appliance).
- Incremental-Only capture for databases that already reside on the array, resulting in faster capture (near-instant) and less storage (no need for a first full copy).
- Highly available mounts from the storage array, coordinated by VDP.
- FC host connectivity with Sky (Actifio Sky to array connection is iSCSI).
- Better scalability of Actifio infrastructure – fewer appliances will be needed, typically.
- Wider support matrix - interop according to the array's connectivity.

Enhanced functionality and usability

Highlights

- Revamped UI for cloud mobility (recovering systems into cloud environments).
- Option to maintain original disk layout during cloud mobility recovery into AWS and GCP.
- Option to map mounted volumes to two ESX hosts, in addition to existing options to mount to one or all ESX hosts in a cluster. This new option provides a faster mount and reduces server volume counts in busy environments.
- Users can now replicate on-demand any snapshot to any remote appliance using StreamSnap incremental replication.
- Additional wizards for Onboarding various databases.
- Enhanced Oracle integration on AppAware mount (TNS listener support, maintain the layout of undo/redo/temp tablespaces).
- Support for managing in-band applications in AGM (this is relevant only for CDS appliances).

Benefits

- AGM provides a single, simple to use interface to manage the entire Actifio environment.
- Enhanced application integration to support a wide variety of customer configuration and use cases.

Enhancements to the Reporting Component

The following are the list of new features and enhancements added in this release:

Real-time Reporting

Actifio Report Manager (RM) administrators can now run real-time reports. Unlike the built-in reports, which look at cached data that is synchronized from the Actifio appliances on a regular schedule, these reports run directly on the Actifio appliances in real-time. The output from each appliance is then combined in the Report Manager to a single spreadsheet or web page.

An extensive list of these real-time reports is available in the RM user interface. Because these have access to data that is not in the RM data cache, these reports often provide information not available elsewhere. These reports can be scheduled and their output can be emailed, saved in the RM repository, or both.

Details on using real-time reporting can be found in the Online help.

Other Enhancements

- A new Cloud Resource Consumption by Day report is added to show resource consumption of snapshot cloud instances.
- Application type names are standardized to match those used in AGM.
- Job reports now show the target OnVault pool to support multiple OnVault targets in a single policy template.
- Job reports now show jobs that copy logs to OnVault.
- The Daily Protection Status report now has its output grouped by policy template instead of by appliance. There are no more empty sections. This leads to much more efficient use of the report's real state.
- Reporting has been added for additional database types: SAP HANA, SAP IQ, SAP ASE, SAP MaxDB, IBM Db2, PostgreSQL, MySQL, and MariaDB.
- A new filter is added to the Unresolved Failures report to allow hiding applications whose scheduler is disabled.

Resolved Issues in AGM 10.0 SP2

The following list summarizes the resolved issue in AGM 10.0 SP2:

Resolved Issues

Issue	Fix	Tracking
AGM		
The Direct Mount workflow page fails to save provisioning parameters when the user changes the selected host.	This issue is now fixed and the provisioning parameters are saved even if user changes the selected host.	84089
AGM UI is enhanced with the additional field in the Help menu to view the AGM API documentation.		87343
AGM UI shows the clone option when the NFS staging option is set for application backup.	This issue is now fixed and the clone option does not show when the NFS staging option is set for application backup.	88243
Sometimes, Move SLA operation fails on VM if imported OnVault images of the same application are present on the source appliance.		83372
Unable to select a source appliance to perform system recovery when OnVault image is imported to multiple appliances.	This issue is now fixed.	86983
Mount operation for the remote Dedup image does not show the image details.		84912

Resolved Issues

Issue	Fix	Tracking
HostAgentMomData character limit caused replication to fail.	This issue is now fixed by increasing the character limit from 32 to a longer value.	87120
AGM upgrade may fail at SchemaHelper while re-calculating the protection status of the application.		82604
VMware discovery fails if ESX's name includes special characters (%).		88423
Profile creation from the AGM CLI fails with an error due to the missing cluster option.	This issue is now fixed and can create a profile with the correct appliance ID option.	86865
While performing the 'Unmount or unmount & delete' operation, for the active images of a grandchild from the Active Mount screen, the screen hung on 'Loading Image Details.'		87631
The Configuring Application Settings for SAP IQ Database Captures screens are enhanced with the buffered block copy option.		84012
Under certain circumstances, active mounts from OnVault images do not show in the ramp view.		84523
The Mount and Migration option was available even when the appliance was an older version.	The option is now available only for appliances 10.0 and later.	84107
AGM UI is enhanced with App Settings for individual group members of the SystemState.		88166
During catalog operation, when an error occurs due to rollback error, an index can be left in an inconsistent state and results in repeated retries.	This issue is now fixed.	83832
Performing the Test failover for the DedupAsync image is failing with error: "Failover is unsuccessful due to Not a mirroring application: 1740771".		86547
Syncback image includes log recovery range details.	This issue is now fixed and now the Syncback image does not include log recovery range details.	87824
The Mapping options for OnVault image are not displayed fully when a SQL CLUSTER VM is selected from the Target list.		83257
SystemState application that is unmanaged and ignored is getting listed when applying the unmanaged filter.		80541
Unable to create a logical group when login user was not part of the organization.	This issue is now fixed.	87686

Resolved Issues

Issue	Fix	Tracking
When a stream snap policy template is cloned, the base snapshot policy id for both original and cloned templates are different.	This issue is now fixed.	86801
On the Job page, the duration of the job is converted from days to hours when downloaded the file in CSV and PDF formats.		87806
Members of a logical group get deleted when a search is performed on the member's grid and saved.		85600
AGM CLI shows data for all organizations even though the user is mapped to a single organization.		86815
Adding an appliance to AGM fails with the error: “Option already exist.”		85091
Consistency Group application, which is marked as sensitive, changes to “No” in the sensitive data column when the application is ignored and vice-versa.	This issue is now fixed.	84055
In certain conditions, Onboarding VM shows the status as failed even though the Onboarding is successful.	This issue is now fixed by adding an Application type filter in the API call.	87637
Google Chrome 84 version rendered error on Mount screens.	This issue is now fixed.	85228
Added field-level help text for the Catalog Search field in the UI.		79250
The Software section in the Appliance health grid is shown in disabled state and zeros.	This issue is now fixed.	86604
Password Management has multiple issues to modify the user interface.	This issue is now fixed.	81666
ESP Unity Job details show the pool type as an Unknown pool type.	This issue is now fixed.	83660
The Appliance page keeps on spinning if the ERROR column is enabled and stale appliances are selected in the global filter.	This issue is now fixed.	88922
AGM’s GET /consistencygroup/{group_id}/ member call fails due to duplicated member entries from the same appliance.	This issue is now fixed.	88981
AGM grids show new data and then switch to old data when multiple API calls run in parallel.	This issue is now fixed.	88702

Resolved Issues

Issue	Fix	Tracking
Logsmart policy migration fails when migration gets executed before the replication starts.	This issue is now fixed.	87369
Staging disk filesystem type does not honor CAF dump backups. Currently, the staging disk filesystem type is picked from the root file system by default.	This issue is now fixed.	88104
AGM+RM upgrade fails as the upgrade process consider the upgrade as RM appliance only.	This issue is now fixed.	87654
CAF log backups are using many staging disks as the default last log staging disk size is set to 10 GB.	This issue is now fixed by increase the default value to be the same as staging disk granularity.	88098
An incorrect error message is displayed when trying to restore mount or migrate with connector versions prior to 10.0.	This issue is now fixed.	84225
Workflows still use NFS, even though the staging disk I/O path is changed from NFS transport to iSCSI.	This issue is now fixed.	86925
In AGM+RM integrated version, Remote Postgres access does not work after upgrading from AGM 8.0.2 to 9.0.2 version and then configuring RM.	This issue is now fixed.	87058
In AGM+RM integrated version, VM is always in the US/Eastern (EST5EDT) time zone after configuration.	This issue is now fixed.	64854
While trying to edit a host that is listed by applying global organization filter throwing an error and loading infinity.	This issue is now fixed.	89014
Duplicate application inventory objects are identified in the VM Onboarding wizard.	This issue is now fixed.	87304
SAML assertion parsing failed while parsing the attributes with the Google SAML IdP setup.	This issue is now fixed.	86474
Unable to update resources of an organization from the Organization page.	This issue is now fixed.	88486
The User screen shows inconsistent timezone.	This issue is now fixed.	80533

Resolved Issues

Issue	Fix	Tracking
AGM replication fails to delete invalid policy option entries that are cleaned up by an Actifio appliance.	This issue is now fixed.	84244 82267
An error occurs when protecting a cluster application that uses external arrays and verification of connectivity from external array to the hosts did not consider the cluster that the application resides on.	This issue is now fixed.	89127
An error is displayed while editing the user information if authentication is disabled.	This issue is now fixed.	87694
AGM API now uses tags for all categories to separate different sections of the APIs.	This issue is now fixed.	87330
Performance issue is observed on AGM when there are millions of job history data.		88590
[Stream Snap]: Access page hangs while using the "Test fail-over" option and shows "loading image details" error.	This issue is now fixed by adding a check for the selected host value.	88251
In the workflow edit screen, the SQL Instance drop-down disables and does not populate any value when the mounted host is changed.	This issue is now fixed.	89230
AGM may lose few records when there are millions of job history data present in it.		85143
Reporting		
The Application Growth report shows incorrect values for OnVault consumption.	This issue is now fixed.	87051
The Resource Consumption report loads the data very slowly in large environments.	This issue is now fixed.	74916
Reports exported to CSV or Excel formats are truncating header text that is not visible.	This issue is now fixed.	87173

5 AGM 10.0 SP1 Enhancements and Resolved Issues

This chapter describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 10.0 SP1 release.

This chapter includes the following topics:

- New Features and Functionality in AGM 10.0 SP1 on page 25
- Resolved Defects in AGM 10.0 SP1 on page 27

For a comprehensive list of known defects in AGM 10.x, see Known Defects on page 45. For a list of CVE fixes, see Security and Vulnerability Issues on page 53.

New Features and Functionality in AGM 10.0 SP1

The following are the new features, enhancements and changes in AGM 10.0 SP1 release:

Test Data Management with Containers

Highlights

Actifio has the ability to make application data accessible from within a container environment. Actifio Virtual Data Pipeline (VDP) technology leverages Kubernetes NFS volumes to make application data available as NFS shares to one or more containers.

Benefits

- Integrating production data into the CI/CD pipeline.
- Data masking.
- Cross-cloud portability.
- Use in on-premise to cloud or cloud to on-premise migration.
- Ability to move application data to another cluster if you exceed your resource capacity.
- Un-mounting and deleting a point-in-time application image when it is not needed.

Streamlined support for SAP IQ and MaxDB

Highlights

- Actifio enhanced its out-of-the-box support for:
    - SAP IQ
    - MaxDB

- Databases are discovered automatically, transaction logs are managed as part of the SLA associated with the databases, and recovery to any point in time and creation of virtual clones are done entirely from the AGM, either on-demand or as part of automated workflows.

Benefits

- Faster deployment and operational simplicity.
- Automated discovery, backup/capture, and recovery of all these databases.
- Log roll forward option to recover databases to any point in time.
- Automated deployment of virtual clones (application aware mount) for TDM use cases.
- No need for using customized scripts - support is out-of-the-box.

Database logs to OnVault

Highlights

- Customers can replicate log backups to OnVault (until now they could only be replicated using StreamSnap).

Benefits

- Customers can use OnVault for DR, especially in the cloud, with very low RPO by replicating logs frequently.
- For remote DevTest use cases, customers can leverage OnVault with more granularity for point-in time data access by rolling logs to a specific point in time.

External Snapshot Pools with Dell EMC Unity

Highlights:

- Actifio has extended its Virtual Data Pipeline to use and manage external snapshot pools with Sky appliances. Customers can leverage their storage arrays' performance, connectivity, and availability by using the array native snapshots for Actifio's snapshot pool. This version adds support for external snapshot pools on Dell EMC Unity arrays.

Benefits:

- Better performance on mounted images. Activity on virtual clones does not go through the Actifio appliance but rather directly between the host and storage array. This is especially important in test/dev environments.
- Better performance and RTO for DR, when using external snapshot pools on the DR side. Data is updated and available in its intended target storage so there is no need to copy it elsewhere.
- Better performance on SmartCopy backups (data moves directly from array to array, without going through an Actifio appliance).
- Incremental-Only capture for application that already reside on the array, resulting in faster capture (nearinstant) and less storage (no need for a first full copy).
- Highly available mounts from the storage array, coordinated by VDP.
- FC host connectivity with Sky (Sky to array connection is iSCSI).
- Better scalability of Actifio infrastructure – fewer appliances will be needed, typically.
- Wider support matrix - interop according to the array's connectivity.

Enhancements to the Reporting Component

The following are the list of new features and enhancements added in this release:

- OnVault replication jobs are now included in the Backup Job details and Unresolved Failures reports.
- When email configurations are changed or updated, you don't need to restart the Tomcat server.
- Added support for SAP HANA, Db2, MySQL, and SAP MaxDB databases.
- The Running Jobs report now supports recovery jobs.
- The Running Jobs report now added with "% Slower Than Previous Durations" filter, where users can create an exception-only report for jobs that are slower than their historic averages.
- The Summary table available in Backup Job Details now includes data copied and a totals row.
- The Unresolved Failures report now tells you when the last successful job occurred for a given application and job type.
- The Snapshot Pool Consumption and Dedup Pool Consumption reports now show consumption details in GB rather than TB.
- Users can now login to RM from AGM using Single Sign-On.

Resolved Defects in AGM 10.0 SP1

The following list summarizes the resolved defects in AGM 10.0 SP1:

Resolved Defects

Issue	Fix	Tracking
AGM		
The Mount and Migration option was available even when the appliance was an older version.	The option is now available only for appliances 10.0 and later.	84107
The list of policies in the Policy Editor and the Template view were out of sync.	The policy list is now synchronized.	83957
In the create and run now workflow pages, the SQL Instance value was not getting updated when a user selected the host.	AGM is listing SQL instance based on the host selection.	83431
An issue with the AGM UI not enforcing the required fields in Advanced Policy Settings page has been fixed.		83713
In the create workflow page, the default Mount Mode option of NFS was not retained once a user enabled the Create New Virtual Application option and made a database selection.	Issue has been fixed.	83203
An issue with missing Map to all cluster node property missing for imported OnVault images has been fixed.		82844
When mounting an image, the vRDM option is not available for selection if the target is a virtual SQL standalone instance.	The vRDM option is now available for selection for virtual SQL standalone instances.	82722

Resolved Defects

Issue	Fix	Tracking
Child application names in the Active Mounts page now have links for easy navigation to the child application's Access view.		82511
The option FORCE FULL FILESYSTEM BACKUP has been removed from the Application Details and Setting page of MariaDB and MySQL applications.		82499
When the number of cataloged indices exceeded a certain limit, user queries were timing out in AGM.	The user query configuration has been extended to twenty minutes, as a result user query no longer times out.	82448
In a very busy system, an error can potentially cause an index to be lost.	Issue has been fixed.	82339
When editing a storage array, the action of removing an appliance was not getting saved. However, AGM was incorrectly showing a success message.	Removal of an appliance when editing a storage array is now successful.	81784
When running a workflow, the Mark Dependent option was showing as disabled even for workflows that were created with an enabled Mark Dependent option.	The Mark Dependent value is displaying accurately.	81653
When running a workflow, the AGM UI was sending incorrect mount mode value.	Issue has been fixed.	81651
When creating a workflow, the mount mode option was resetting to the default vault value of NFS when the user enabled the Create New Virtual Application option.	The mount mode is no longer resetting to the default value.	81647
AGM user could not add SSH key for CLI access when using LDAP group authentication.	Issue has been fixed.	81530
Added multi-byte character support for username in AGM.		81289
When running a workflow, the AGM UI was not respecting the transport mode on the host.	Issue has been fixed.	81285
A new property "Hana Target Node" has been added to the restore page for SAP HANA applications. This drop-down option allows the user to select a node name from the node list. It is available only when cluster type is 'SAPHANA Replication Cluster'.		80806
A new property "SAPHANA Replication Cluster" is available in the Application Details and Settings page for the SAP HANA applications.		80568
Log roll forward option was allowed for images on which log was already replayed.	Issue has been fixed and the user will no longer see the log range populated if the log has already replayed.	80556

Resolved Defects

Issue	Fix	Tracking
During a mount operation, if a VMWare standalone host is selected as the Target host, the AGM UI was not honoring the host transport mode.	The host transport mode is honored.	80240
In the table view of the Access page (in Application Manager), the Clone option is not available for File System applications.		81052
Added membership support for PostgreSQL applications.		80126
The image details section of SAP HANA applications show the backup capture method configured for the application. Options are "Full+incremental backup" or "Volume level backup".		80042
AGM users with non administrator permission can now view a list of completed jobs of an application if the application belongs to the same organization as the host. Previously, they were restricted to viewing jobs with the status "Running".		79664, 79545
When a host is assigned to organization, non-admin users belongs to that organization with roles like manage and run SLA for applications on that host were not able to see completed jobs in System Monitor.	Issue has been fixed.	79645
The Restore filter in System Monitor page now lists job of type remote restore.		79414
AGM users were forced to change their password any time they needed to update their email address or timezone.	AGM users are no longer prompted to change their password when updating their email address or timezone.	78040
For SAP ASE applications, users can enter either the password or the file path in the Edit Host for application discovery.		71732
Reporting		
In the integrated version, logical groups added to an organization in AGM does not include its members in RM's organization.	Issue has been fixed.	82560
Schedule reports do not show data properly when the email schedule timezone is different from the Report Manager timezone.	Issue has been fixed.	80136
Daily Protection reports do not show StreamSnap jobs when its schedule settings are not inherited from the Snapshot policy.	Issue has been fixed.	79296
Resource Consumption by Organization report does not show data when the current day is selected.	Issue has been fixed.	77571

Resolved Defects

Issue	Fix	Tracking
In the integrated version, Actifio Report Manager (RM) will sync appliance IP from Actifio Global Manager (AGM) even though the same IP already exists in RM.	Issue has been fixed.	77284

6 AGM 10.0 Enhancements and Resolved Issues

This chapter describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 10.0.0 release.

This chapter includes the following topics:

- New Features and Functionality in AGM 10.0 on page 31
- Resolved Defects in AGM 10.0 on page 36
- VDP Features and Functions Not Supported in AGM 10.0 on page 43

For a comprehensive list of known defects in AGM 10.x, see Known Defects on page 45. For a list of CVE fixes, see Security and Vulnerability Issues on page 53.

New Features and Functionality in AGM 10.0

The following are the new features, enhancements and changes in AGM 10.0 release:

Enhanced Actifio Global Manager (AGM) functionality and usability

Highlights

Actifio is transitioning to Actifio Global Manager for all appliance and data management. This version adds the following functionality and usability enhancements to AGM:

- o Revamped, consolidated menu structure to make it easier for users to carry out main tasks such as backup and recovery, as well as TDM capture and access.
- o An interactive "guided tour" to acquaint users with the main UI sections.
- o Wizards for application onboarding and data recovery.
- o Streamlined support for SAP HANA, SAP ASE (formerly Sybase ASE), Db2, and MySQL.
- o Integrated Report Manager as part of AGM deployment - one VM to deploy, ease of launching RM from AGM, and synchronized users, organizations, and appliances to reduce redundant configurations.
- o Complete support for managing Hyper-V VMs
- o Enhanced handling of logical groups and organizations
- o Global prune paths for file system applications
- o Ability to clone SLA templates

Benefits

AGM provides a single, simple to use interface to manage the entire Actifio environment.

- Support for NFS with HP-UX and AIX servers

Usability and Performance Enhancements

Actifio is transitioning to using Actifio Global Manager for all appliance and data management. This version adds the following "parity" functionality and usability enhancements to AGM.

- Support for databases and other generic applications on Linux using the change-block tracking driver.
- Ability to export the content displayed in various grids (application list, host list, etc.) to CSV or PDF files.
- Streamlined display and management of application details & settings, including showing defaults and easily restoring defaults.
- User can easily look up job failure errors in ActifioNOW knowledge base, directly from System Monitor job details.
- All table displays use a consistent grid component with standard, rich functionality.
- Easy "short-cut" application list to move between applications when looking at an application page (e.g., Manage SLA, Access).

Highlights

AGM provides a single interface to manage the entire VDP environment.

Cloud VM snapshots (10.0 SP)

Highlights

Customers can leverage native cloud snapshots to protect their AWS and GCP cloud instances. Operationally, the same SLA-based simplicity that customers have come to expect from Actifio is provided, in combination with using native cloud snapshots for easy and fast recovery. Customers can recover disks into existing instances, as well as clone or restore the entire instance. No Actifio connector is required for these operations.

Benefits

Simple protection of cloud instances, without needing to install a connector.

Fast recoveries, as snapshots are available immediately for reads.

CDX (in mainstream code, with other 9.0 functionality)

Highlights

CDX 10c is on the same code stream as Sky and CDS, meaning it has substantially all the functionality of 10c (and 9.0, since the previous CDX release was 8.1.2). This includes NFS support, external snapshot pools, multi-target OnVault, and the rest of the 10c features in this document.

Note that data mounted over NFS does not remain available upon CDX node failure.

Benefits

All the previous benefits of CDX, including high availability, FC support, performance, etc.

Near-zero downtime recovery for SQL Server and file systems (Mount & Migrate)

Highlights

Further enhancing Actifio's leadership in recovery speed, customers can now recover SQL Server and file system data instantly using Actifio's existing capabilities and in addition migrate the data in real-time to production storage, while the application is up and running.

Actifio customers have always benefited from the ability to instantly mount their backups, regardless of data set size, and be able to get their applications up and running. However, if they needed to move recovered data into some other storage (local server or SAN storage), that required some downtime for the data migration period. The new capability in 10c eliminates that need and migrates the data while the applications are up and running, thereby allowing completion of the full recovery process with almost no downtime. Recovery can be back to the original location or to another server. This gives DBAs and backup administrators the same capability that VMware admins have had for years by using Storage vMotion to move a mounted VM from Actifio to their production storage while the VM is running.

Benefits

Provide a near-zero RTO for data recovery back to the final storage destination.

Shorten downtime for server and storage migrations

OnVault to multiple targets (introduced in 9.0.2)

Highlights

Application data can now be sent to multiple OnVault targets, on-premise or in the cloud.

Each OnVault target is controlled by separate policies so frequency of update and retentions can be different (e.g., frequent local updates with short retention, together with less frequent updates to cloud with long-term retention).

Multi-target OnVault is supported with all application types, including Direct-to-OnVault with VMware VMs. In the latter case, the data is written directly to the first OnVault pool, bypassing the snapshot pool, and then read from the first OnVault pool and sent to the others.

Benefits

Flexibility for multiple use cases. For example, customers can protect the data locally, keep it for long retention remotely in one cloud, and send data to another cloud for TDM purposes. Customers can also send the data to multiple clouds to avoid reliance on one cloud vendor.

OnVault rehydration performance & incremental options

Highlights

The performance of a mount from OnVault has been enhanced by using any blocks that are currently available in the snapshot pool instead of reading them from object storage. This is similar to the incremental rehydration with dedup where only blocks that are not in the snapshot pool get rehydrated from dedup.

When performing a mount from OnVault the user will have options to control how much they want to optimize for performance vs. storage consumption, by selecting from the following:

- Storage-optimized: only keep writes in the local snapshot pool (writes are always kept locally).
- Balanced: blocks that are read (from object storage) or written (to local snapshot pool) are kept in the snapshot pool, to serve as a "cache" for future reads.
- Performance-optimized: bring the entire image to the local snapshot pool, in the background. Reads will become faster as more of the image is available locally.
- Max performance: The entire image is rehydrated into the snapshot pool first, prior to the mount. This means that the host always works against local storage only.

Benefits

Enhanced performance from object storage, enabling the use of applications that can benefit from, or require higher performance similar to that of local storage.

Streamlined support for SAP HANA, SAP ASE, IBM Db2, MySQL, MariaDB

Highlights

Actifio enhanced its out-of-the-box support for:

- SAP HANA, SAP ASE (formerly Sybase ASE), and IBM Db2 as of VDP 9.0.3
- MySQL as of VDP 9.0.4
- MariaDB as of VDP 10.0
- SAP IQ (formerly Sybase IQ) planned for 10.0.1.

Databases are discovered automatically, transaction logs are managed as part of the SLA associated with the databases, and recovery to any point in time and creation of virtual clones are done entirely from the AGM, either on-demand or as part of automated workflows.

Benefits

Faster deployment and operational simplicity.

Automated discovery, backup/capture, and recovery of all these databases.

Log roll forward option to recover databases to any point in time.

Automated deployment of virtual clones (application aware mount) for TDM use cases.

No need for using customized scripts - support is out-of-the-box.

OnVault to Dell EMC PowerProtect DD for long-term retention

Highlights

Customers can use their Dell EMC PowerProtect DD (formerly Data Domain) infrastructure as OnVault targets for long-term retention. User defines an OnVault pool with a PowerProtect DD target and all other OnVault functionality is as usual.

Direct to OnVault is supported (for VMware VMs) as well as OnVault replication (from one pool to another).

Customer can set PowerProtect DD to replicate to another PowerProtect DD system. This is not controlled from Actifio, but images on the replication target system can be imported into an Actifio appliance, similarly to how it would be done with a regular OnVault pool. Before importing, the replication between the two PowerProtect DD systems must be stopped and the data on the target system must be designated as read/write.

DD Boost technology is used to minimize the data sent from the Actifio appliance to PowerProtect DD.

Benefits

Customers can leverage their investment in Data Domain infrastructure, combined with all Actifio's capabilities.

Enhanced support for SQL Server Always-on Availability Groups

Highlights

User can specify dynamic rules for handling databases within the AAG, similar to existing functionality for SQL Server Instances (all, system, user, include/exclude specific databases).

User can further control and define rules for the selection of AAG node to be used for backup (primary, secondary, etc.).

Benefits

Enhanced automation and usability requires less admin work.

Fast replication of any snapshot image using StreamSnap

Highlights

In addition to the existing StreamSnap policy that can replicate snapshot images according to a pre-defined SLA, user can now replicate on demand any snapshot image between two Actifio appliances. Replication is done from the local snapshot pool to the remote snapshot pool in an incremental fashion, relative to the latest dated remote snapshot image.

Benefits

Enhanced data portability on demand.

Other AGM Enhancements

- Nginx web certificate is now complaint with the latest regulations:

  Due to the security constraints enforced by the CA/Browser Forum and some major vendors, the Web TLS certificate on this appliance will be validated on a daily basis.

  Note: *Please disregard this message if either a commercial or enterprise certificate is installed on your appliance.*

  If a self-signed Web TLS certificate is used (which is the default), and it does not comply with the security constraints or it is set to expire in seven (7) days, it will automatically be replaced by a new self-signed certificate. The web server on the appliance will be restarted and your browser will need to be refreshed before it works with the new certificate. You will see security warnings prompting you to refresh your browser.

- A backup admin user with a profile configured to use an OnVault pool could occasionally encounter a frozen "Manage SLA" page when creating a template with onvault policy. This happened if the user's profile did not have onvault pool selected in his or her Organization.

  Instead of a frozen screen, user now sees an error, similar to the following example: `Diskpool with srcid 915441 does not exist on the appliance with clusterid 1415093150`. (Bug 77709)

- Users list page lists a new "Local Auth" column. The value in the column is 'Yes' or 'No' to indicate whether the user is authenticated locally. (Bug 76351)
- AGM CLI has been enhanced so that the lsapplication command can interpret "volumes" in a user friendly format. (Bug 74560)
- Move SLA functionality has been added for Hyper-V applications. (Bug 74538)
- A more efficient full text or keyword search has been implemented to improve responsiveness of searches involving keywords. (Bug 74104)
- When deleting templates, profiles, applications, host and backup images from AGM, the Tombstone records are now retained for three (3) days. (Bug 73962)
- Backup image metadata lists optional attributes backedupdb, skippeddb and faileddb. (Bug 73400)
- Downloaded jobs list files contain dates in long format. (Bug 73373)
- AGM search now has an option for exact match to find specific LDAP groups quickly. (Bug 63075)
- AGM has a new access permission, "Catalog Access" that allows non-administrator AGM users to access and use Catalog functionality. (Bug 62748)
- Logical Groups can be added for managed applications. (Bug 66005)
- A new API has been introduced to push an SLA template to an appliance from AGM. (Bug 66265)

Enhancements to the Reporting Component

The following are the list of new features and enhancements added in this release:

- The emails generated by scheduled reports can now include the DNS name for Report Manager instead of just the IP address.
- The Audit Trail Report by Appliance now supports filtering audit records by user name, audit details, and privileged or unprivileged commands.
- New reports added in this release:
  - Application Growth
  - Database Log Backup Summary
- System state recovery jobs are now included in the Recovery Job Details and Recovery JobSummary reports.
- The Restorable Images report now shows the mounted host name.
- Report Manager now supports storing the database partition on LVM to simplify growing thepartition if it fills up.
- Recovery Job Details Report supports running jobs.
- Resource Consumption Reports support OnVault consumption.
- Now you can filter multiple patterns of host and application names using the boolean 'OR' between the search criteria.
- The reporting engine is upgraded to a new version.

Resolved Defects in AGM 10.0

The following list summarizes the resolved defects in AGM 10.0:

Resolved Defects

Issue	Fix	Tracking
AGM		
Resolved an issue that prevented user selected datastore from being used during VM restores initiated through AGM.		78902
Catalog search results were incorrectly displayed in Internet Explorer.	Catalog search results now display correctly in Internet Explorer.	78401
AGM users were forced to change their password any time they needed to update their email address or timezone.	An AGM user is no longer forced to change password when updating email address or timezone.	78040
AGM was not showing the policies associated with an SLA Template created in an appliance.	AGM now shows all policies for an SLA Template that are created in an appliance.	77567

Resolved Defects

Issue	Fix	Tracking
In a search results grid, the footer displayed the text "Matching: " followed by the search text. This was misleading because the displayed results were also affected by the filters applied in the other columns, and were not a true reflection of the search results.	The text "Matching: " followed by the search text is no longer displayed in the footer of the search results grid.	77503
When trying to protect a SQL database that is part of an Instance, the AGM user will now see a message: `The selected application belongs to SQL Instance. Click OK to navigate to Manage SLA for the SQL Instance.`		77191
Dedup options section for dedup and remote dedup images was missing from the mount page.	Issue has been fixed.	76877
AGM user with Workflow Run ACL right can view and run workflows.		76356
When protecting a child SQL application, the option to backup only the database was missing.	The option to backup only the database is now available.	75988
Background activity to refresh the UI was preventing inactive user sessions in AGM from timing out.	AGM user session now times out unless there is explicit user activity.	75868
When replicating data to multiple object storage pools on older appliances running 8.0.x, a backward compatibility issue was identified. The AGM UI was trying to update the multi-OnVault policy with newer properties that were not supported on the appliance.	Applying multi-OnVault policy templates to older appliances will return the following message: Policy update is not successful on all the appliances associated. Change is persisted on AGM.sky-8-0-7: errormessage: invalid option: targetvault errorcode: 10010. Note: Replicating data to multiple object Storage Pools capability was introduced in AGM 9.0.3 and appliances that are older than AGM 9.0.2 are not compatible.	75817
Fixed an issue that was preventing some administrator users from accessing sensitive data..		75717
Listing applications for an Organization with a large Resource Membership resulted in a Server Request Failed error.	Issue has been fixed.	75111
AGM pages were in a loading state after adding an IQN with quotes at the end.	An error message is shown to the user when the invalid format is supplied.	74894
RDM mount options are now available for Generic App (LVM) applications.		74888

Resolved Defects

Issue	Fix	Tracking
Login credential options were available for Oracle database servers with OS authentication configuration.	Login credentials are available only when the Oracle servers are configured for database authentication and when the database role is standby/secondary.	74855
AGM was showing host as well as application metadata even after the host and its applications were deleted from the appliance.	Issue has been fixed and AGM no longer shows metadata related to deleted hosts and applications.	74853
Updating an SLA could take a long time.	Improvements have been made to update an SLA faster.	74716
The Clone action has now been removed for all custom application framework (CAF) applications.		74251
Syncback images were incorrectly getting listed in the Remote Snapshot lane of the Timeline Ramp view.	Syncback images are now listed in the Snapshot lane.	74175
For an application discovered in multiple appliances, AGM was creating duplicated policyoption entries when pushing the new app-only option to multiple appliances simultaneously.	Issue has been fixed and no duplicate entries are created.	73879
When editing a host, AGM now displays an error message if an invalid WWPN port number or a duplicate iSCSI port number is provided.		73785
AGM was allowing LDAP mapping to the PUBLIC organization resulting in complications.	AGM will throw an error if user tries to map an LDAP group to the PUBLIC organization.	73687
An issue has been resolved in handing cluster Ids larger than 2147483647. Previously, cluster IDs with a large numerical value resulted in error messages in AGM like "java.lang.NumberFormatException: For input string "2517693698"".		73656
In certain situations where AGM was managing a large number of appliances (over 100) and data replications were parallel, AGM was deadlocked in the UdsIdGenerator due to massive concurrent database access.	The ID generation has been improved to prevent the deadlocks. In addition, the hibernate connection pool max_size has been updated from 25 to 50.	73384
Issue with OutOfMemoryError exception in the Java heap after upgrading to AGM 9.0.4 has been resolved.		73306
Trying to mark a Consistency Group as ignored or sensitive was returning the error message: 'Cannot delete protected application'.	Issue has been fixed and AGM user can mark a Consistency Group as ignored or sensitive.	73267

Resolved Defects

Issue	Fix	Tracking
When editing a Dedup Async template, the user was seeing intervals in hours instead of minutes even when the interval was specific in minutes.	The interval is now correctly showing up as minutes if it had been saved as minutes.	73259
For HP-UX applications, AGM users can now modify the Staging Disk Format property from Block to NFS and from NFS to Block.		73257
App Manager Listing page is enhanced with pop up messages for SQL Instance and Consistency Group protection.		72621
Trying to clone SteamSnap image of a SQL application resulted in page loading error.	Issue has been fixed. After loading the Clone screen, users are now presented a dropdown list to choose host. Once a host has been selected, cloning of SQL application image completes successfully.	72418
The Remote Snapshot image associated with previous StreamSnap is listed immediately. Previously, it could take upto fifteen (15) minutes to show up.		72045
The Direct Mount and LiveClone workflow pages preserve the provisioning option values when a new target host is selected.		71854
VMware 6.7 Update 3 and higher cannot deploy Actifio OVA files due to VMware's decision to implement a different hashing algorithm and block the previous one. Actifio OVA files can be converted using the VMware tool "ovftool" to change SHA1 to SHA256, and then users could deploy the OVA files.	Actifio OVA files now use SHA256.	71834
Resolved an issue with multi-page lists when filters change in a way that results in the user being on a page beyond the end of the results.		71333
The error message displayed on insufficient user privileges now has a new title “Insufficient Access Privileges”. Previously, the title used to be “Insufficient Rights”.		71331
When editing an On-Demand workflow, the Frequency property is no longer displayed as it is not applicable to On-Demand workflows.		71129
When mounting an application, AGM warned the user to select the Mount Mode as pRDM, even though the option was not appropriate.	The AGM UI prompts user to select the Mount Mode as pRDM only when appropriate.	71123
Editing a user detail like organization was overwriting or deleting other metadata ,such as the key for CLI access.	The CLI access key is no longer deleted or overwritten when other user details are updated.	71083
AGM timeout issues when deleting an SLA have been resolved.		70728

Resolved Defects

Issue	Fix	Tracking
Patch files uploaded via Internet Explorer 11 would fail due to unnecessary file path information. The upload process included additional file path information, as a result of which AGM was unable to validate the incoming file.	AGM no longer includes the additional file path information.	70554
When searching for Cataloged data, the error message that was returning after supplying an invalid date range was not meaningful.	As a result of enhancements to Catalog search capability, the invalid date range scenario is no longer an issue.	70503
When running a re-provision job, AGM now displays a couple of new statuses to indicate what jobs it is running. The status messages "Workflow Mount Task Running" and "Workflow LiveClone Task Running" have been added.		70344
The AGM Workflow APIs have been modified to support the refreshing of an existing virtual application with simpler payload. Previously, the Run WorkFlow API required complete workflow details to refresh a virtual application. It now requires only the name to refresh.		70092
Issue with high CPU usage by the AGM System Monitor service has been fixed,		70062
User was able to create a Dedup-Async Replication (DAR) Production to Mirror policy with an empty "Every" field. Subsequently however, managing an application with that policy failed.	The Every property no longer accepts a zero (0) or non numeric value. If the user clears the property text box, it will retain the previously assigned value.	69823
AGM was not allowing users to perform the restore operation from a remote dedup image.	Restore can now be successfully performed from remote dedup images.	69702
An issue has been fixed with usage of temporary tables to prevent them from growing indefinitely.		69463
The `lspolicyoption` command in AGM CLI command was not allowing users to use "name" as a valid `filtervalue` attribute.	Issue has been fixed.	69123
Application aware mount for a LiveClone image is now successful when an application is enabled for log backups.		69372
NFS options did not pick up multiple IP addresses.	Issue has been fixed.	69142
On the 'Manage SLA' page for an Application belonging to a Managed Logical Group, the 'Apply SLA...' button is now visible and disabled. Previously the button was showing up as enabled.		68405

Resolved Defects

Issue	Fix	Tracking
During an upgrade, the user saw the login to AGM message while the upgrade was still in progress.	AGM login page does not show prematurely.	68374
When creating or editing a template in the AGM UI, the Scheduling > Windowed configuration was accepting zero, negative and non-numeric values.	Issue is now fixed.	68200
Password restriction rules are now enforced for administrator users as well.		68174
Host matching/consolidation across appliances has been enhanced to be case insensitive when all other identifiers match.		68147
AGM is now capable of saving Oracle workflows with SLT and SLP for newly provisioned App-aware mounts.		67044
In the 'Create Profile' page, the term used to identify the remote appliance has now been reverted back to 'Remote Appliance'. It was previously referred to as 'Primary Remote'.		66932
If user deleted some templates, AGM would be unable to replicate these template deletions to the appliance, failing with an internal error.	This issue has been addressed, and template deletions get correctly replicated to the appliance.	66536
When creating a Profile, AGM allows user to choose only those OnVault pools that are defined for the target appliance.		66543
VM clusters that were previously not showing in AGM are now visible.		65525
AGM allows user names with special characters: @, #, %, ',' and $ to comply with the character set allowed by LDAP. For example: jane.doe, @janedoe, and so on.		65500
Unable to create a user with a blank password for a new LDAP user.	User can create a blank password for a new LDAP user.	66317
In the Manage SLA page, for unmanaged applications and consistency groups, 'Apply SLA' button has now been renamed to "Apply SLA…". Clicking this button brings up the Apply SLA dialog box. Withing this dialog box, the "Save" button has been renamed to "Apply SLA".		65398
Using the VM onboarding wizard, the AGM user can protect multiple VMs with the same SLA.		64989
Application discovery initiated from AGM by a non-admin user now succeeds even when the organization assignments in AGM and the appliance are not in sync.		64644
A new column "Mount Type" has been added to the Active Images page. It is not shown by default but users can configure the column settings to view the column.		64640

Resolved Defects

Issue	Fix	Tracking
Mounted images did not show which appliance was providing the mount.	The Mount Appliance column in the Active Mount page shows the appliance name.	64638
In a multi-hop configuration, AGM failed to perform on-demand backup and returned the message "'"Failed to start backup, policy must belong to application's SLA".	On-demand backup jobs are successful in multi-hop configurations.	64587
The pRDM and vRDM options for edit workflow page were missing for workflows that were created in a version of AGM prior to 8.1.3.	The pRDM and vRDM options have been added to provide backward compatibility with workflows created in versions of AGM prior to 8.1.3.	64565
New filter option 'Disabled Only' has been added to list applications where manage expiration feature is disabled. Additionally, a new column 'Expirations Enabled' has been added. This column is hidden by default. It will show the value "Yes" if an application has enabled image expiration, and show the value "No" if an application has disabled expirations.		64180
Improved performance of SQL Failover instances containing many files when the network connection between cluster hosts is slow.		63910
Provisioning a template to other appliances from AGM was failing if the template had policy options that were unknown to the AGM.	Issue has been fixed.	63803
The Organizations panel in the LDAP Group Mapping page was showing an empty list when more than one hundred (100) organizations were defined in AGM.	The Organization panel now lists all organizations.	62861
Permissions issue with AGM using a role to run a workflow. Host Manage right was required to run workflows.	Issue has been fixed. User can now run workflows without the host manage right.	62520
The Job Details page in AGM System Monitor has a new filter option "Oracle ASM Rebalance". It replaces three filter options AGM had in prior releases: "ASM Rebalance", "ASM Switch", and "ASM Switch Undo".		62447
When adding a host for the first time from Domain Manager in AGM, if there were more then eleven (11) appliances available to add, then some of them did not get listed in the Appliances section of the Add Host page. This was because AGM limited the number of available hosts to eleven from the add or edit host pages for the very first time.	The add host page now lists all available appliances.	62347
In the Applications List page, new filter options 'Template Name' and 'Profile Name' have been added to help search for templates and profiles by name.		61889
OnVault images have a new "Ownership" property that can be set to Yes or No.		61491

Resolved Defects

Issue	Fix	Tracking
Issue with the missing OnVault Pool column in the SLA Architect's Profile page has been fixed.		61477
Updating the Resource Profile for a managed Logical Group showed a success message even when there was an error saving the profile.	AGM now displays an error message if there is any error saving the updated resource profile.	61140
The Event Id details that was missing in the job details page are now available.		58212
AGM allows users to perform "Unmount & Delete" for backup images mounted to Azure cloud.		57057
Selecting job number in the System Monitor was not refreshing the job details.	Job details get refreshed.	55374
After a fresh install, AGM was forcing users to add an appliance before the user could perform any action.	AGM users are no longer forced to add an appliance. They can configure user role and perform other actions as needed.	54932
Attempting to remove a policy from a template in AGM resulted in a 10053 error - Provisioning operation not performed, waiting for cluster lock.	Policies can now be deleted from templates in AGM.	50358
The `Error Code <Code>` metadata is available for Status column in the Jobs list page.		45968
The Catalog search page has an option to cancel the search.		43459
Reporting		
Administrative user with multiple roles assigned can now see all the data in Report Manager.		79513
The Failed Jobs report now includes re-provision job types.		65620

VDP Features and Functions Not Supported in AGM 10.0

AGM 10.0 supports most of the features and functions available in the recent VDP releases. Features and functions not currently supported by AGM 10.0 can be performed at the VDP Desktop.

The following list summarizes the features and functions that are not part of AGM 10.0.

- **Multi-Hop Replication to Address Complex Backup Replications**: Replicate remote dedup backups to another site by adding a second "leg" of replication between VDP appliances.
- **NAS Director Support**: Management of large unstructured data stored on EMC Isilon Scale Out NAS systems by a VDP appliance. This capability leverages the native APIs from EMC Isilon to efficiently capture changed file data, eliminating the scanning of file systems to determine the changed files.

7 Known Defects

This section describes the known defects in the Actifio Global Manager (AGM) 10.0 release. It includes the following topics:

Known Defects in AGM 10.0.5

The following list summarizes the known defects in AGM 10.0.5:

Known Defects

Issue	Workaround	Tracking
AGM		
[Oracle only]: Database restore on Remote Dedup image fails.	Initiate restore using table view and then select the remote dedup image.	88288
The Cloud Instances of AWS and GCP are not available in the Application Capture Wizard at this time.	Issue will be fixed in a future release.	84281
Following an upgrade, the AGM UI shows service menu icons from prior AGM versions (AGM 9.0.x) on some browsers. This is happening because the browser is retaining some of the older interfaces in its cache.	To workaround the issue, clear the browser cache.	79763
For HMC hosts, the “Discover Applications” section (where users can add login information and port number of the HMC host) in the Edit host page is not available.	Issue will be fixed in a future release.	78226
From the Manage tab in the AGM Dashboard, the appliance connectivity status is showing as stale even though all the services were running without any issues in the appliance.	Issue will be fixed in a future release.	71867
UNIX utilities such as grep and less are not available to users in the AGM CLI.	Issue individual commands via SSH and use local utilities on a client host if they are needed	71045

Known Defects

Issue	Workaround	Tracking
Saving a consistency group with 2,000 databases can take more than a few minutes.	Issue will be fixed in a future release.	63706
When upgrading AGM deployed on Hyper-V, the user may see the login to AGM screen while the upgrade is still in progress.	Wait for some time (twenty minutes approximately), to let the upgrade process finish. Then login to the upgraded AGM.	62203
With certain paired appliances in sharing mode, an edge case defect exists such that an application cannot be protected. This can happen only in the scenario where the AGM manages both the master and the slave appliance.	Appliances managed by AGM should be joined in non-sharing mode.	56636
Applying a File Catalog enabled policy to a Catalog ineligible application (like databases) will result in the system ignoring the File Catalog function.	Fix will be available in a future release.	44700
When you remove an appliance from an AGM which has Catalog functionality enabled, AGM will disable future scanning of the appliance. If you add the appliance back to an AGM with Catalog, applications that were cataloged before the appliance was removed will resume scanning and indexing. However, AGM will not be able to use the metadata anymore. AGM will use metadata only from the newly-managed applications that have cataloging enabled.	No known workaround. Further enhancements are planned in a subsequent release.	41868
VMware guest tools may not start after an AGM upgrade.	If you require VMware guest tools, contact your Actifio support representative.	37095
Actifio 7.1.0 CDS and Sky appliances that were not upgraded to Hot Fix 1199 or later can generate an error when imported to AGM. Example error: • Template: snaponly • Policy: snap • Field: iscontinuousincoming value: trueexisting value: null Hot Fix 1099 addressed issues associated with policies with window duration longer than 23 hours and 50 minutes with a schedule type of daily.	To resolve this issue, you must remove AGM's conflicting policies, apply HotFix 1199 to the Actifio appliance, and then re-import the Actifio 7.1.0 appliance to AGM.	37041

Known Defects

Issue	Workaround	Tracking
If an Actifio appliance managed by AGM is experiencing network issues, AGM can take several minutes to load an application list. This is because AGM cannot tell if the Actifio appliance is disconnected or is just slow. After waiting a few minutes, AGM will mark the Actifio appliance as Stale, and the application list page performance will return to normal. **Note:** *If the Actifio appliance is going through a normal maintenance window, AGM will immediately identify the appliance as Stale and the performance of the application list page will remain normal.* In addition, when the issue with a Stale Actifio appliance is resolved, AGM will delay up to 10 minutes to report the new status of the Actifio appliance.	If you are experiencing performance issues with application lists, or if you believe the status of an Actifio appliance has changed from Stale to Normal, but AGM is still showing it as Stale. Please wait at least 10 minutes. If 10 minutes or more have passed and the performance of application lists is still slow, or the Actifio appliance in question is still marked as Stale, contact Actifio Customer Support.	36820
When multiple Organizations are selected from the Organizations page under the Manage tab: • The Edit and Delete options are both active; however, editing multiple Organizations is not allowed. You can only edit one Organization at a time. • The Delete option does not delete all of the selected Organizations. Only the last selected Organization is deleted.	Do not use the Edit option when multiple Organizations are selected. When you need to delete multiple Organizations, delete one Organization at a time.	36443
If two Actifio appliances are joined and set to Sharing Mode, if you add the Primary as well as Secondary Appliances, you MUST add the Primary appliance first. After both appliances are added, updated templates can be pushed to both appliances. When the Primary receives an updated template, it will push the updated template to the Secondary. Because both AGM and the Primary will push the same updated template to the Secondary appliance, it may result in an error.	These errors are benign and can be ignored.	35482
If you are using a Microsoft Internet Explorer web browser with the AGM UI, you may experience one or more of the following issues outlined below: • The AGM UI will intermittently fail to display all LDAP mappings due to an Internet Explorer browser incompatibility. [25947] • The AGM version number in the lower left-hand corner is not immediately displayed when viewing in Internet Explorer. ssIf you redirect the cursor to another area in the lower left-hand corner, then the version number will appear. [30466]	If you find that you are experiencing one or more of the issues outlined above, we recommend switching to a different browser such as Google Chrome or Mozilla Firefox to use the AGM UI.	30466, 25947

Known Defects

Issue	Workaround	Tracking
When you perform an Unmount and Delete operation for an active image in the Active Images window, in some cases, you may still see the mount image. The Active Image list does not refresh the table after performing an unmount or delete operations and shows invalid operations as a result.	Refresh the Active Image list, and the appropriate operations will be shown.	28419
During the AGM software upgrade process, you may encounter the error message "Unpacking file is currently in progress. Please try again later.".	If you see the error message, click **OK** to close the popup window and perform a screen refresh. Retry the AGM software upgrade procedure as outlined in the AGM Online Help System.	23873
After you add an appliance to AGM, Actifio recommends not to create additional policy templates on the imported appliance. Templates created on an appliance that is already imported will be displayed in the AGM user interface, but cannot be managed by AGM. These "unmanaged" templates can only be managed from the appliance on which they were created.[	For SLA Templates that were created on an appliance after it has been imported to AGM: The name of each post-import policy template is appended with the originating appliance name, and the renamed template is visible in the Manage Templates view (for example, T1_abc will be renamed T1_abc_SQA122CT). However, when a job is viewed in the Jobs view of System Monitor, AGM will display the original name of the SLA template (for example, T1_abc) because the job information is read from the VDP appliance. Keep in mind that these two SLA templates, although slightly different in name, are the same post-import policy template. When you create a new template in the SLA Architect on the VDP appliance, the appliance initially names it with a generic name (for example, New Template12). If AGM synchronizes with the VDP appliance before you have a chance to rename the policy template, AGM will add the template with the generic name and append it with the appliance name (for example, New Template12_SQA122CT).	22747

Known Defects

Issue	Workaround	Tracking
The Applications window in the App Manager is missing additional application-specific information such as Priority, Other Nodes, Protected Data, Host IP Address, and Unique Name, similar to what can be viewed in the App Manager from the VDP Desktop	Issue will be fixed in a future release.	24439, 24449, 24442, 24410
During importing, logical group-to-organization assignments on the imported VDP appliance will not be imported to AGM. For example, if there is a logical group named “group1” on VDP Appliance 1, which is assigned to “organization1,” after importing VDP Appliance 1 to AGM “group1” on AGM will lose its organization assignments. It will only be visible to the admin user on AGM.	Actifio recommends that you review all imported logical groups after importing and, if necessary, reassign them to the proper organizations.	22138
VDP appliance users imported with CLI access rights will not be flagged with having this access right in AGM. The CLI Access field in the Users window of AGM identifies if a user has the proper rights to access the AGM CLI. This field does not specify if that user has CLI access rights to the VDP appliance CLI.	You will still need to enable the VDP appliance CLI usage rights and access from the VDP Desktop.	20710
If the VM on the source VDP appliance is added as in-band for data storage, and you move the management of that VM to a target VDP appliance, after the VM is moved it will be added as out-of-band on the target appliance. This occurs because the target VDP appliance is not aware of the in-band LUN(s) on the source VDP appliance.	No known workaround.	20533

Known Defects

Issue	Workaround	Tracking
The management of application copy data involves AGM pushing a copy of SLA templates to the VDP appliances responsible for managing the applications. If, at a future point in time, you make additional updates to an AGM-managed SLA template, and there is a communication failure during the push of the updated template to a VDP appliance, AGM will be unable to complete the push of the updated template to this appliance. In this case, the SLA template will become out-of-sync between AGM and the VDP appliance and this template discrepancy can result in an SLA violation.	You will be notified when a communication failure occurs between AGM and its managed VDP appliances. If you experience a communication failure during a push of an updated SLA template, we recommend that you make the same set of updates to the SLA template and save those changes. AGM will again attempt to push the updated SLA template to the VDP appliances responsible for managing the applications, including the appliance that experienced the original network failure. If the retry still fails, we recommend that you investigate and resolve the source communication problem, and then perform a retry until the SLA template is in sync between AGM and the VDP appliance. [20430]	20430
When performing a PrepMount operation for a LiveClone image, when you view the Prep Mount image in the Active Images window the Original Backup name is left blank.	This behavior is due to the fact that the Original backup name would be the actual name of the LiveClone image itself.	18362
When AGM and Appliance are in different timezone, appliance time is displayed in Image card details (in the Ramp view) and AGM timezone in tear drop.	No known workaround. Issue will be fixed in a future release.	87982
After successful upgrade from AGM 10.0.0 to AGM 10.0.2 using Firefox box browser, clicking the 'log back into AGM' link displays a blank page instead of log in page.	Close the Firefox browser window and clear the cache to load the AGM properly.	89359
Oracle DB restore fails for Remote Dedup image.	No known workaround. Issue will be fixed in a future release.	88288
Data inclusion rule changes after the mount and migrate of SQL instance.	Change the rule and re-apply the old rule from manage SLA.	85967
Reporting		
Schedules created on standalone Report Manager by superuser fail to run after migrating to an integrated version.	Recreate the schedules on the integrated version.	81518

Known Defects

Issue	Workaround	Tracking
Changes made to saved options do not affect existing scheduled jobs.	Create a new schedule.	62791
The header text disappears from every page after page 1 when column header is to set filter or sort order.	No known workaround. Issue will be fixed in a future release.	86376
The Application Details section of the Snapshot Pool Consumption report does not include external snapshot pool data.	No known workaround. Issue will be fixed in a future release.	62958
For Job History Summary by Application Report, the totals will count DB+log backups as two jobs (a log backup and a snapshot) even though there is just 1 job record.	No known workaround.	53938
User cannot apply column filter to show rows which do not have any information.	No known workaround. Issue will be fixed in a future release.	52034
When a report is scheduled with different timezone other than RM system timezone, it shows incorrect values for Start Time and End Time in the scheduled Report.	No known workaround. This is a third party issue: JS-32957.	31889
Tool-tip and drill-down functionality in line charts does not work properly when default zoom level (100%) is changed.s	No known workaround.	27933
Daily Protection Status report has some issues with horizontal scrolling in HTML view.	No known workaround.	27713
Actifio Report Manager does not work properly if your browser is configured with an ad-blocking extension (uBlock).	Disable/delete the browser extensions.	25857
PDF report download fails with Google Chrome browser.	Use Save as PDF option in print menu or you may use another browser to download the PDF.	--
If an external user (VDP appliance users) does not have any applications associated or there is no data available for the selected criteria, the following two reports are not displayed. [RM-133] • SLA Violation Summary • SLA Violation Summary for last 24 hours	No known workaround. This is a known third-party issue with dual pie-charts.	Third-party case no.00065485
Actifio Report Manager shows incorrect system time when upgraded to a 10.x version from 9.x versions.	Root access is required to change the system time, contact Actifio Support.	91404

Known Defects

Issue	Workaround	Tracking
In Report Manager, any saved filters or schedules for the following reports that explicitly include the job type "log-backup" will not work properly after upgrade: o Backup Job Details o Failed Jobs o Job History Summary by Application o Unresolved Failures. The job type "log-backup" will no longer be selected.	Update the filter or schedule to include the job type "Log Backup".	243918842
On an application protected with streamsnap policy, restoring to a different target with the "replace original application identity" option, shows the SLA and backup images before restore, as associated with the original source application even after a successful restore.	Remove streamsnap protection before running restore with 'replace original application identity'. This issue is not applicable for restores that do not use "replace original application identity' option".	244709301
Report Manager displays the error "JSON schema validation failed: params: Invalid type: string (expected object)" when you click the refresh button twice.	Click the **Apply** button at the bottom of the Input Controls in the left panel.	249686572
When recovering a VMware VM into Google Cloud, the guest OS hostname is being set equal to the recovered VM name, and this may result in databases and applications inside the VM failing to start if it is different than it was in the source environment.	When recovering a VMware VM into Google Cloud, specify to use the original hostname as the new VM name.	248981679
Application discovery fails, when trying to discovery using IP address.	Add the host to the AGM and try discovering the application.	269060261

8 Security and Vulnerability Issues

This section lists security and vulnerability (CVEs) fixes. It includes the following topics:

Security Fixes in AGM 10.0 SP5

The following security issues were fixed in AGM 10.0 SP5:

Security Fixes

Description	CESA#
CentOS update for wget centos7	CESA-2019:1228
CentOS: security advisory for libxml2	CESA-2021:3810, CESA-2020:3996
CentOS: security advisory for nss	CESA-2020:4076, CESA-2021:4904
CentOS: security advisory for ppp	CESA-2020:0630
CentOS: security advisory for python	CESA-2022:5235, CESA-2020:5009
CentOS: security advisory for screen	CESA-2021:0742
CentOS update for nss-softokn centos7	CESA-2019:4190
CentOS update for nss-util centos7	CESA-2019:4190
CentOS: security advisory for bpftool	CESA-2021:3801, CESA-2021:0856, CESA-2021:1071, CESA-2021:2314, CESA-2021:2725, CESA-2021:3438, CESA-2021:4777, CESA-2022:4642, CESA-2020:5437, CESA-2022:0620, CESA-2020:3220, CESA-2021:3327, CESA-2020:5023, CESA-2022:0063, CESA-2020:2664
CentOS: security advisory for cyrus-sasl	CESA-2022:0666

Security Fixes

Description	CESA#
CentOS: security advisory for expat	CESA-2022:1069
CentOS: security advisory for icu	CESA-2020:0897
CentOS: security advisory for iwl1000-firmware	CESA-2021:0339
CentOS: security advisory for lemon	CESA-2020:0227
CentOS: security advisory for microcode_ctl	CESA-2021:3028
CentOS: security advisory for bind	CESA-2020:2344, CESA-2021:0671, CESA-2020:5011, CESA-2021:1469
CentOS: security advisory for perl	CESA-2021:0343
CentOS: security advisory for binutils	CESA-2021:4033
CentOS: security advisory for grub2	CESA-2020:3217
CentOS: security advisory for nettle	CESA-2021:1145
CentOS: security advisory for aide	CESA-2022:0473
CentOS: security advisory for curl	CESA-2020:5002
CentOS: security advisory for polkit	CESA-2022:0274
CentOS: security advisory for bsdcpio	CESA-2020:0203
CentOS: security advisory for glib2	CESA-2021:2147
CentOS: security advisory for java	CESA-2021:2845
CentOS: security advisory for ldb-tools	CESA-2021:1072
CentOS: security advisory for minizip	CESA-2022:2213
CentOS: security advisory for openldap	CESA-2022:0621
CentOS: security advisory for openssl	CESA-2021:3798, CESA-2022:1066, CESA-2020:5566
CentOS: security advisory for dhclient	CESA-2021:2357
CentOS: security advisory for ntp	CESA-2020:2663
CentOS: security advisory for openssh	CESA-2021:4782

Security Fixes

Description	CESA#
CentOS: security advisory for rpm	CESA-2021:4785
CentOS: security advisory for dbus	CESA-2020:2894
entOS: security advisory for kernel	CESA-2022:0063
CentOS: security advisory for microcode_ctl	CESA-2020:2432, CESA-2020:5083
CentOS: security advisory for java	CESA-2021:1298, CESA-2022:0306, CESA-2022:1487, CESA-2022:5698, CESA-2020:2968
CentOS: security advisory for gzip	CESA-2022:2191
CentOS: security advisory for xz	CESA-2022:5052
CentOS update for java-11-openjdk centos7	CESA-2021:2784
CentOS update for freetype centos7	CVE-2020-15999
CentOS update for wpa_supplicant centos7	CESA-2021:0808

CVEs Fixed in AGM 10.0 SP5

The following Common Vulnerabilities and Exposures (CVEs) were fixed in AGM 10.0 SP5:

Resolved CVEs

Description	CVE #
libxml2, possibly before 2.5.0, does not properly detect recursion during entity expansion, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, aka the "billion laughs attack."	CVE-2003-1564
jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.	CVE-2012-6708

Resolved CVEs

Description	CVE #
org.apache.http.conn.ssl.AbstractVerifier in Apache HttpComponents HttpClient before 4.3.5 and HttpAsyncClient before 4.0.2 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a "CN=" string in a field in the distinguished name (DN) of a certificate, as demonstrated by the "foo,CN=www.apache.org" string in the O field.	CVE-2014-3577
jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.	CVE-2015-9251
Remote code execution occurs in Apache Solr before 7.1 with Apache Lucene before 7.1 by exploiting XXE in conjunction with use of a Config API add-listener command to reach the RunExecutableListener class. Elasticsearch, although it uses Lucene, is NOT vulnerable to this. Note that the XML external entity expansion vulnerability occurs in the XML Query Parser which is available, by default, for any query request with parameters deftype=xmlparser and can be exploited to upload malicious data to the /upload request handler or as Blind XXE using ftp wrapper in order to read arbitrary local files from the Solr server. Note also that the second vulnerability relates to remote code execution using the RunExecutableListener available on all affected versions of Solr.	CVE-2017-12629
A deserialization flaw was discovered in the jackson-databind in versions before 2.8.10 and 2.9.1, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper. This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.	CVE-2017-15095
FasterXML jackson-databind through 2.8.10 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the Spring libraries are available in the classpath.	CVE-2017-17485
The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2003-1564.	CVE-2017-18640
A deserialization flaw was discovered in the jackson-databind, versions before 2.6.7.1, 2.7.9.1 and 2.8.9, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper.	CVE-2017-7525
Fasterxml Jackson version Before 2.9.8 contains a CWE-20: Improper Input Validation vulnerability in Jackson-Modules-Java8 that can result in Causes a denial-of-service (DoS). This attack appear to be exploitable via The victim deserializes malicious input, specifically very large values in the nanoseconds field of a time value. This vulnerability appears to have been fixed in 2.9.8.	CVE-2018-1000873
Swagger UI before 4.1.3 could allow a remote attacker to conduct spoofing attacks. By persuading a victim to open a crafted URL, an attacker could exploit this vulnerability to display remote OpenAPI definitions.	CVE-2018-25031

Resolved CVEs

Description	CVE #
X-Pack Machine Learning versions before 6.2.4 and 5.6.9 had a cross-site scripting (XSS) vulnerability. Users with manage_ml permissions could create jobs containing malicious data as part of their configuration that could allow the attacker to obtain sensitive information from or perform destructive actions on behalf of other ML users viewing the results of the jobs.	CVE-2018-3823
X-Pack Machine Learning versions before 6.2.4 and 5.6.9 had a cross-site scripting (XSS) vulnerability. If an attacker is able to inject data into an index that has a ML job running against it, then when another user views the results of the ML job it could allow the attacker to obtain sensitive information from or perform destructive actions on behalf of that other ML user.	CVE-2018-3824
Elasticsearch Alerting and Monitoring in versions before 6.4.1 or 5.6.12 have an information disclosure issue when secrets are configured via the API. The Elasticsearch _cluster/ settings API, when queried, could leak sensitive configuration information such as passwords, tokens, or usernames. This could allow an authenticated Elasticsearch user to improperly view these details.	CVE-2018-3831
FasterXML jackson-databind through 2.8.11 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 and CVE-2017-17485 deserialization flaws. This is exploitable via two different gadgets that bypass a blacklist.	CVE-2018-5968
Apache Commons Configuration performs variable interpolation, allowing properties to be dynamically evaluated and expanded. The standard format for interpolation is "${prefix:name}", where "prefix" is used to locate an instance of org.apache.commons.configuration2.interpol.Lookup that performs the interpolation. Starting with version 2.4 and continuing through 2.7, the set of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote servers. These lookups are: - "script" - execute expressions using the JVM script execution engine (javax.script) - "dns" - resolve dns records - "url" - load values from urls, including from remote servers Applications using the interpolation defaults in the affected versions may be vulnerable to remote code execution or unintentional contact with remote servers if untrusted configuration values are used. Users are recommended to upgrade to Apache Commons Configuration 2.8.0, which disables the problematic interpolators by default.	CVE-2022-33980
FasterXML jackson-databind before 2.7.9.3, 2.8.x before 2.8.11.1 and 2.9.x before 2.9.5 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the c3p0 libraries are available in the classpath.	CVE-2018-7489
A vulnerability was found in Infinispan such that the invokeAccessibly method from the public class ReflectionUtil allows any application class to invoke private methods in any class with Infinispan's privileges. The attacker can use reflection to introduce new, malicious behavior into the application.	CVE-2019-10174

Resolved CVEs

Description	CVE #
A series of deserialization vulnerabilities have been discovered in Codehaus 1.9.x implemented in EAP 7. This CVE fixes CVE-2017-17485, CVE-2017-7525, CVE-2017-15095, CVE-2018-5968, CVE-2018-7489, CVE-2018-1000873, CVE-2019-12086 reported for FasterXML jackson-databind by implementing a whitelist approach that will mitigate these vulnerabilities and future ones alike.	CVE-2019-10202
A vulnerability was found in Hibernate-Validator. The SafeHtml validator annotation fails to properly sanitize payloads consisting of potentially malicious code in HTML comments and instructions. This vulnerability can result in an XSS attack.	CVE-2019-10219
jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	CVE-2019-11358
A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint, the service has the mysql-connector-java jar (8.0.14 or earlier) in the classpath, and an attacker can host a crafted MySQL server reachable by the victim, an attacker can send a crafted JSON message that allows them to read arbitrary local files on the server. This occurs because of missing com.mysql.cj.jdbc.admin.MiniAdmin validation.	CVE-2019-12086
FasterXML jackson-databind 2.x before 2.9.9.1 might allow attackers to have a variety of impacts by leveraging failure to block the logback-core class from polymorphic deserialization. Depending on the classpath content, remote code execution may be possible.	CVE-2019-12384
A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x through 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has JDOM 1.x or 2.x jar in the classpath, an attacker can send a specifically crafted JSON message that allows them to read arbitrary local files on the server.	CVE-2019-12814
SubTypeValidator.java in FasterXML jackson-databind before 2.9.9.2 mishandles default typing when ehcache is used (because of net.sf.ehcache.transaction.manager.DefaultTransactionManagerLookup), leading to remote code execution.	CVE-2019-14379
A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9.2. This occurs when Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the logback jar in the classpath.	CVE-2019-14439
A flaw was discovered in jackson-databind in versions before 2.9.10, 2.8.11.5 and 2.6.7.3, where it would permit polymorphic deserialization of a malicious object using commons-configuration 1 and 2 JNDI classes. An attacker could use this flaw to execute arbitrary code.	CVE-2019-14892

Resolved CVEs

Description	CVE #
A flaw was discovered in FasterXML jackson-databind in all versions before 2.9.10 and 2.10.0, where it would permit polymorphic deserialization of malicious objects using the xalan JNDI gadget when used in conjunction with polymorphic type handling methods such as \`enableDefaultTyping()\` or when @JsonTypeInfo is using \`Id.CLASS\` or \`Id.MINIMAL_CLASS\` or in any other way which ObjectMapper.readValue might instantiate objects from unsafe sources. An attacker could use this flaw to execute arbitrary code.	CVE-2019-14893
A flaw was found in Hibernate ORM in versions before 5.3.18, 5.4.18 and 5.5.0.Beta1. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SELECT or GROUP BY parts of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks.	CVE-2019-14900
A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to com.zaxxer.hikari.HikariDataSource. This is a different vulnerability than CVE-2019-14540.	CVE-2019-16335
Netty before 4.1.42.Final mishandles whitespace before the colon in HTTP headers (such as a "Transfer-Encoding : chunked" line), which leads to HTTP request smuggling.	CVE-2019-16869
A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the commons-dbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of org.apache.commons.dbcp.datasources.SharedPoolDataSource and org.apache.commons.dbcp.datasources.PerUserPoolDataSource mishandling.	CVE-2019-16942
A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the p6spy (3.8.6) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of com.p6spy.engine.spy.P6DataSource mishandling.	CVE-2019-16943
A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLookup.	CVE-2019-17267
A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the apache-log4j-extra (version 1.2.x) jar in the classpath, and an attacker can provide a JNDI service to access, it is possible to make the service execute a malicious payload.	CVE-2019-17531
FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.	CVE-2019-20330
HttpObjectDecoder.java in Netty before 4.1.44 allows an HTTP header that lacks a colon, which might be interpreted as a separate header with an incorrect syntax, or might be interpreted as an "invalid fold."	CVE-2019-20444
HttpObjectDecoder.java in Netty before 4.1.44 allows a Content-Length header to be accompanied by a second Content-Length header, or by a Transfer-Encoding header.	CVE-2019-20445

Resolved CVEs

Description	CVE #
jQuery-UI is the official jQuery user interface library. Before version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to refuse the value of the `altField` option from untrusted sources.	CVE-2021-41182
A permission issue was found in Elasticsearch versions before 5.6.15 and 6.6.1 when Field Level Security and Document Level Security are disabled and the _aliases, _shrink, or _split endpoints are used . If the elasticsearch.yml file has xpack.security.dls_fls.enabled set to false, certain permission checks are skipped when users perform one of the actions mentioned above, to make existing data available under a new index/alias name. This could result in an attacker gaining additional permissions against a restricted index.	CVE-2019-7611
A race condition flaw was found in the response headers Elasticsearch versions before 7.2.1 and 6.8.2 returns to a request. On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.	CVE-2019-7614
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.aries.transaction.jms.internal.XaPooledConnectionFactory (aka aries.transaction.jms).	CVE-2020-10672
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.caucho.config.types.ResourceRef (aka caucho-quercus).	CVE-2020-10673
A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.	CVE-2020-10693
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.aoju.bus.proxy.provider.remoting.RmiProvider (aka bus-proxy).	CVE-2020-10968
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to javax.swing.JEditorPane.	CVE-2020-10969
In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	CVE-2020-11022
In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	CVE-2020-11023

Resolved CVEs

Description	CVE #
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.activemq.* (aka activemq-jms, activemq-core, activemq-pool, and activemq-pool-jms).	CVE-2020-11111
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.proxy.provider.remoting.RmiProvider (aka apache/commons-proxy).	CVE-2020-11112
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.openjpa.ee.WASRegistryManagedRuntime (aka openjpa).	CVE-2020-11113
The ZlibDecoders in Netty 4.1.x before 4.1.46 allow for unbounded memory allocation while decoding a ZlibEncoded byte stream. An attacker could send a large ZlibEncoded byte stream to the Netty server, forcing the server to allocate all of its free memory to a single decoder.	CVE-2020-11612
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.springframework.aop.config.MethodLocatingFactoryBean (aka spring-aop).	CVE-2020-11619
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.jelly.impl.Embedded (aka commons-jelly).	CVE-2020-11620
An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.	CVE-2020-13936
Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URIs passed to the library as java.net.URI object and pick the wrong target host for request execution.	CVE-2020-13956
FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to oadd.org.apache.xalan.lib.sql.JNDIConnectionPool (aka apache/drill).	CVE-2020-14060
FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to oracle.jms.AQjmsQueueConnectionFactory, oracle.jms.AQjmsXATopicConnectionFactory, oracle.jms.AQjmsTopicConnectionFactory, oracle.jms.AQjmsXAQueueConnectionFactory, and oracle.jms.AQjmsXAConnectionFactory (aka weblogic/oracle-aqjms).	CVE-2020-14061
FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to com.sun.org.apache.xalan.internal.lib.sql.JNDIConnectionPool (aka xalan2).	CVE-2020-14062

Resolved CVEs

Description	CVE #
FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to org.jsecurity.realm.jndi.JndiRealmFactory (aka org.jsecurity).	CVE-2020-14195
Bouncy Castle BC Java before 1.66, BC C# .NET before 1.8.7, BC-FJA before 1.0.1.2, 1.0.2.1, and BC-FNA before 1.0.1.1 have a timing issue within the EC math library that can expose information about the private key when an attacker is able to observe timing information for the generation of multiple deterministic ECDSA signatures.	CVE-2020-15522
FasterXML jackson-databind 2.x before 2.9.10.6 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.AnterosDBCPDataSource (aka Anteros-DBCP).	CVE-2020-24616
FasterXML jackson-databind 2.x before 2.9.10.6 mishandles the interaction between serialization gadgets and typing, related to com.pastdev.httpcomponents.configuration.JndiConfiguration.	CVE-2020-24750
A flaw was found in hibernate-core in versions prior to and including 5.4.23.Final. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SQL comments of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. The highest threat from this vulnerability is to data confidentiality and integrity.	CVE-2020-25638
A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.	CVE-2020-25649
An issue was discovered in PlayJava in Play Framework 2.6.0 through 2.8.2. The body parsing of HTTP requests eagerly parses a payload given a Content-Type header. A deep JSON structure sent to a valid POST endpoint (that may or may not expect JSON payloads) causes a StackOverflowError and Denial of Service.	CVE-2020-27196
This affects the package com.fasterxml.jackson.dataformat:jackson-dataformat-cbor from 0 and before 2.11.4, from 2.12.0-rc1 and before 2.12.1. Unchecked allocation of byte buffer can cause a java.lang.OutOfMemoryError exception.	CVE-2020-28491
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.datasources.PerUserPoolDataSource.	CVE-2020-35490
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.datasources.SharedPoolDataSource.	CVE-2020-35491
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.oracle.wls.shaded.org.apache.xalan.lib.sql.JNDIConnectionPool (aka embedded Xalan in org.glassfish.web/javax.servlet.jsp.jstl).	CVE-2020-35728

Resolved CVEs

Description	CVE #
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to oadd.org.apache.commons.dbcp.cpdsadapter.DriverAdapterCPDS.	CVE-2020-36179
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.cpdsadapter.DriverAdapterCPDS.	CVE-2020-36180
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.cpdsadapter.DriverAdapterCPDS.	CVE-2020-36181
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.cpdsadapter.DriverAdapterCPDS.	CVE-2020-36182
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.docx4j.org.apache.xalan.lib.sql.JNDIConnectionPool.	CVE-2020-36183
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.datasources.PerUserPoolDataSource.	CVE-2020-36184
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp2.datasources.SharedPoolDataSource.	CVE-2020-36185
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.datasources.PerUserPoolDataSource.	CVE-2020-36186
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.tomcat.dbcp.dbcp.datasources.SharedPoolDataSource.	CVE-2020-36187
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.newrelic.agent.deps.ch.qos.logback.core.db.JNDIConnectionSource.	CVE-2020-36188
FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.newrelic.agent.deps.ch.qos.logback.core.db.DriverManagerConnectionSource.	CVE-2020-36189
jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.	CVE-2020-36518

Resolved CVEs

Description	CVE #
Elasticsearch versions before 6.8.13 and 7.9.2 contain a document disclosure flaw when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries. This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.	CVE-2020-7020
Elasticsearch versions before 7.10.0 and 6.8.14 have an information disclosure issue when audit logging and the emit_request_body option is enabled. The Elasticsearch audit log could contain sensitive information such as password hashes or authentication tokens. This could allow an Elasticsearch administrator to view these details.	CVE-2020-7021
Netty 4.1.43.Final allows HTTP Request Smuggling because it mishandles Transfer-Encoding whitespace (such as a [space]Transfer-Encoding:chunked line) and a later Content-Length header. This issue exists because of an incomplete fix for CVE-2019-16869.	CVE-2020-7238
jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.	CVE-2020-7656
FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.	CVE-2020-8840
A temp directory creation vulnerability exists in all versions of Guava, allowing an attacker with access to the machine to potentially access data in a temporary directory created by the Guava API com.google.common.io.Files.createTempDir().	CVE-2020-8908
When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.	CVE-2020-9484
Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender. Fixed in Apache Log4j 2.12.3 and 2.13.1.	CVE-2020-9488
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.hadoop.shaded.com.zaxxer.hikari.HikariConfig (aka shaded hikari-config).	CVE-2020-9546
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.ibatis.sqlmap.engine.transaction.jta.JtaTransactionConfig (aka ibatis-sqlmap).	CVE-2020-9547

Resolved CVEs

Description	CVE #
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.AnterosDBCPConfig (aka anteros-core).	CVE-2020-9548
A flaw was found in jackson-databind before 2.9.10.7. FasterXML mishandles the interaction between serialization gadgets and typing. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	CVE-2021-20190
The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package "jquery-validation". jquery-validation before version 1.19.3 contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This is fixed in 1.19.3.	CVE-2021-21252
Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty before version 4.1.59.Final there is a vulnerability on Unix-like systems involving an insecure temp file.	CVE-2021-21290
Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty (io.netty:netty-codec-http2) before version 4.1.60.Final there is a vulnerability that enables request smuggling.	CVE-2021-21295
In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.	CVE-2021-22096
Spring Security 5.4.x prior to 5.4.4, 5.3.x prior to 5.3.8.RELEASE, 5.2.x prior to 5.2.9.RELEASE, and older unsupported versions can fail to save the SecurityContext if it is changed more than once in a single request.A malicious user cannot cause the bug to happen (it must be programmed in). However, if the application's intent is to only allow the user to run with elevated privileges in a small portion of the application, the bug can be leveraged to extend those privileges to the rest of the application.	CVE-2021-22112
The vulnerability is that IDToken verifier does not verify if token is properly signed. Signature verification makes sure that the token's payload comes from valid provider, not from someone else. An attacker can provide a compromised token with custom payload. The token will pass the validation on the client side. We recommend upgrading to version 1.33.3 or above.	CVE-2021-22573
This affects all versions before 10.1.14 and from 10.2.0 to 10.2.4 of package com.typesafe.akka:akka-http-core. It allows multiple Transfer-Encoding headers.	CVE-2021-23339
In Eclipse Jetty 9.4.37.v20210219 to 9.4.38.v20210224, the default compliance mode allows requests with URIs that contain %2e or %2e%2e segments to access protected resources within the WEB-INF directory. For example a request to /context/%2e/WEB-INF/web.xml can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application.	CVE-2021-28164
In OWASP CSRFGuard through 3.1.0, CSRF can occur because the CSRF cookie may be retrieved by using only a session token.	CVE-2021-28490

Resolved CVEs

Description	CVE #
A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.	CVE-2021-30640
Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honored the identity encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.	CVE-2021-33037
An XXE issue in SAXBuilder in JDOM through 2.0.6 allows attackers to trigger a denial of service via a crafted HTTP request.	CVE-2021-33813
For Eclipse Jetty versions 9.4.37-9.4.42, 10.0.1-10.0.5 & 11.0.1-11.0.5, URIs can be crafted using some encoded characters to access the content of the WEB-INF directory and/or bypass some security constraints. This is a variation of the vulnerability reported in CVE-2021-28164/GHSA-v7ff-8wcx-gmc5.	CVE-2021-34429
When reading a specially crafted 7Z archive, the construction of the list of codecs that decompress an entry can result in an infinite loop. This could be used to mount a denial of service attack against services that use Compress' sevenz package.	CVE-2021-35515
When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.	CVE-2021-35516
When reading a specially crafted TAR archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' tar package.	CVE-2021-35517
When reading a specially crafted ZIP archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' zip package.	CVE-2021-36090
When reading a specially crafted TAR archive an Apache Ant build can be made to allocate large amounts of memory that finally leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	CVE-2021-36373
When reading a specially crafted ZIP archive, or a derived formats, an Apache Ant build can be made to allocate large amounts of memory that leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Commonly used derived formats from ZIP archives are for instance JAR files and many office files. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	CVE-2021-36374

Resolved CVEs

Description	CVE #
The Bzip2 decompression decoder function doesn't allow setting size restrictions on the decompressed output data (which affects the allocation size used during decompression). All users of Bzip2Decoder are affected. The malicious input can trigger an OOME and so a DoS attack.	CVE-2021-37136
The Snappy frame decoder function doesn't restrict the chunk length which may lead to excessive memory usage. Beside this it also may buffer reserved skippable chunks until the whole chunk was received which may lead to excessive memory usage as well. This vulnerability can be triggered by supplying malicious input that decompresses to a very big size (via a network stream or a file) or by sending a huge skippable chunk.	CVE-2021-37137
All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.	CVE-2021-40690
Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.	CVE-2021-41079
jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the \`altField\` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the \`altField\` option is now treated as a CSS selector. A workaround is to not accept the value of the \`altField\` option from untrusted sources.	CVE-2021-41182
jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various "*Text" options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various "*Text" options are now always treated as pure text, not HTML. A workaround is to not accept the value of the "*Text" options from untrusted sources.	CVE-2021-41183
jQuery-UI is the official jQuery user interface library. Before version 1.13.0, accepting the value of the \`of\` option of the \`.position()\` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the \`of\` option is now treated as a CSS selector. A workaround is to refuse the value of the \`of\` option from untrusted sources.	CVE-2021-41184
In Apache MINA, a specifically crafted, malformed HTTP request may cause the HTTP Header decoder to loop indefinitely. The decoder assumed that the HTTP Header begins at the beginning of the buffer and loops if there is more data than expected. Please update MINA to 2.1.5 or greater.	CVE-2021-41973
The fix for bug 63362 present in Apache Tomcat 10.1.0-M1 to 10.1.0-M5, 10.0.0-M1 to 10.0.11, 9.0.40 to 9.0.53 and 8.5.60 to 8.5.71 introduced a memory leak. The object introduced to collect metrics for HTTP upgrade connections was not released for WebSocket connections once the connection was closed. This created a memory leak that, over time, could lead to a denial of service via an OutOfMemoryError.	CVE-2021-42340

Resolved CVEs

Description	CVE #
In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.	CVE-2021-42550
Akka HTTP 10.1.x before 10.1.15 and 10.2.x before 10.2.7 can encounter stack exhaustion while parsing HTTP headers, which allows a remote attacker to conduct a Denial of Service attack by sending a User-Agent header with deeply nested comments.	CVE-2021-42697
Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. Netty prior to version 4.1.71.Final skips control chars when they are present at the beginning / end of the header name. It should instead fail fast as these are not allowed by the spec and could lead to HTTP request smuggling. Failing to do the validation might cause netty to "sanitize" header names before it forward these to another remote system when used as proxy. This remote system can't see the invalid usage anymore, and therefore does not do the validation itself. Users should upgrade to version 4.1.71.Final.	CVE-2021-43797
The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client.	CVE-2021-43980
Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.	CVE-2021-44228
Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.	CVE-2021-44832
It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.	CVE-2021-45046
Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.	CVE-2021-45105

Resolved CVEs

Description	CVE #
In Eclipse Jetty versions 9.4.0 thru 9.4.46, and 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, the parsing of the authority segment of an http scheme URI, the Jetty HttpURI class improperly detects an invalid input as a hostname. This can lead to failures in a Proxy scenario.	CVE-2022-2047
pgjdbc is the offical PostgreSQL JDBC Driver. A security hole was found in the jdbc driver for postgresql database while doing security research. The system using the postgresql library will be attacked when attacker control the jdbc url or properties. pgjdbc instantiates plugin instances based on class names provided via \`authenticationPluginClassName\`, \`sslhostnameverifier\`, \`socketFactory\`, \`sslfactory\`, \`sslpasswordcallback\` connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. This can lead to code execution loaded via arbitrary classes. Users using plugins are advised to upgrade. There are no known workarounds for this issue.	CVE-2022-21724
In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.	CVE-2022-22950
A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.	CVE-2022-22965
In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.	CVE-2022-22970
In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.	CVE-2022-22971
The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability into Apache Tomcat 10.1.0-M1 to 10.1.0-M8, 10.0.0-M5 to 10.0.14, 9.0.35 to 9.0.56 and 8.5.55 to 8.5.73 that allowed a local attacker to perform actions with the privileges of the user that the Tomcat process is using. This issue is only exploitable when Tomcat is configured to persist sessions using the FileStore.	CVE-2022-23181
There's a vulnerability within the Apache Xerces Java (XercesJ) XML parser when handling specially crafted XML document payloads. This causes, the XercesJ XML parser to wait in an infinite loop, which may sometimes consume system resources for prolonged duration. This vulnerability is present within XercesJ version 2.12.1 and the previous versions.	CVE-2022-23437
ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library. Prior to version 2.3.0.0, the default implementation of \`Validator.getValidDirectoryPath(String, String, File, boolean)\` may incorrectly treat the tested input string as a child of the specified parent directory. This potentially could allow control-flow bypass checks to be defeated if an attack can specify the entire string representing the 'input' path. This vulnerability is patched in release 2.3.0.0 of ESAPI. As a workaround, it is possible to write one's own implementation of the Validator interface. However, maintainers do not recommend this.	CVE-2022-23457

Resolved CVEs

Description	CVE #
Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.	CVE-2022-24785
Netty is an open-source, asynchronous event-driven network application framework. The package `io.netty:netty-codec-http` prior to version 4.1.77.Final contains an insufficient fix for CVE-2021-21290.	CVE-2022-24823
ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library. Prior to version 2.3.0.0, there is a potential for a cross-site scripting vulnerability in ESAPI caused by a incorrect regular expression for "onsiteURL" in the **antisamy-esapi.xml** configuration file that can cause "javascript:" URLs to fail to be correctly sanitized. This issue is patched in ESAPI 2.3.0.0. As a workaround, manually edit the **antisamy-esapi.xml** configuration files to change the "onsiteURL" regular expression. More information about remediation of the vulnerability, including the workaround, is available in the maintainers' release notes and security bulletin.	CVE-2022-24891
If a web application sends a WebSocket message concurrently with the WebSocket connection closing when running on Apache Tomcat 8.5.0 to 8.5.75 or Apache Tomcat 9.0.0.M1 to 9.0.20, it is possible that the application will continue to use the socket after it has been closed. The error handling triggered in this case could cause a pooled object to be placed in the pool twice. This could result in subsequent connections using the same object concurrently which could result in data being returned to the wrong use and/or other errors.	CVE-2022-25762
The package org.yaml:snakeyaml from 0 and before 1.31 are vulnerable to Denial of Service (DoS) due missing to nested depth limitation for collections.	CVE-2022-25857
** DISPUTED ** In pgjdbc before 42.3.3, an attacker (who controls the jdbc URL or properties) can call java.util.logging.FileHandler to write to arbitrary files through the loggerFile and loggerLevel connection properties. An example situation is that an attacker could create an executable JSP file under a Tomcat web root. NOTE: the vendor's position is that there is no pgjdbc vulnerability; instead, it is a vulnerability for any application to use the pgjdbc driver with untrusted connection properties.	CVE-2022-26520
moment is a JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of moment were found to use an inefficient parsing algorithm. Specifically using string-to-date parsing in moment (more specifically rfc2822 parsing, which is tried by default) has quadratic (N^2) complexity on specific inputs. Users may notice a noticeable slowdown is observed with inputs above 10k characters. Users who pass user-provided strings without sanity length checks to moment constructor are vulnerable to (Re)DoS attacks. The problem is patched in 2.29.4, the patch can be applied to all affected versions with minimal tweaking. Users are advised to upgrade. Users unable to upgrade should consider limiting date lengths accepted from user input.	CVE-2022-31129

Resolved CVEs

Description	CVE #
jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-site scripting. Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. Calling `.checkboxradio( "refresh" )` on such a widget and the initial HTML contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery UI 1.13.2. To remediate the issue, someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.	CVE-2022-31160
PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using standard, database independent Java code. The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of column names so a malicious column name that contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL commands as the application's JDBC user. User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that do invoke that method are impacted if the underlying database that they are querying via their JDBC application may be under the control of an attacker. The attack requires the attacker to trick the user into executing SQL against a table name who's column names would contain the malicious SQL and subsequently invoke the `refreshRow()` method on the ResultSet. Note that the application's JDBC user and the schema owner need not be the same. A JDBC application that executes as a privileged user querying database schemas owned by potentially malicious less-privileged users would be vulnerable. In that situation it may be possible for the malicious user to craft a schema that causes the application to execute commands as the privileged user. Patched versions will be released as `42.2.26` and `42.4.1`. Users are advised to upgrade. There are no known workarounds for this issue.	CVE-2022-31197
The Apache Xalan Java XSLT library is vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode. The Apache Xalan Java project is dormant and in the process of being retired. No future releases of Apache Xalan Java to address this issue are expected. Note: Java runtimes (such as OpenJDK) include repackaged copies of Xalan.	CVE-2022-34169
Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache XML Graphics allows an attacker to load a url thru the jar protocol. This issue affects Apache XML Graphics Batik 1.14.	CVE-2022-38398
Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache XML Graphics allows an attacker to fetch external resources. This issue affects Apache XML Graphics Batik 1.14.	CVE-2022-38648
Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.	CVE-2022-38749
Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.	CVE-2022-38750
Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.	CVE-2022-38751

Resolved CVEs

Description	CVE #
Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack-overflow.	CVE-2022-38752
Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache XML Graphics allows an attacker to access files using a Jar url. This issue affects Apache XML Graphics Batik 1.14.	CVE-2022-40146
CSRF tokens in Spring Security are vulnerable to a breach attack. Spring Security always returns the same CSRF token to the browser.	WS-2016-7107
Affected versions of the package are vulnerable to Directory Traversal, which may allow access to sensitive files and data on the server.	WS-2017-3734
Vue.js before 2.5.17 vesion in vue poject have potential xss in ssr when using v-bind.	WS-2018-0162
Apache commons-codec before version "commons-codec-1.13-RC1" is vulnerable to information disclosure due to Improper Input validation.	WS-2019-0379
Inclusion of Functionality from Untrusted Control Sphere vulnerability found in jcommander before 1.75. jcommander resolving dependencies over HTTP instead of HTTPS.	WS-2019-0490
Spring Security before 5.2.9, 5.3.7, and 5.4.3 vulnerable to side-channel attacks. Vulnerable versions of Spring Security don't use constant time comparisons for CSRF tokens.	WS-2020-0293
An issue was found in all versions of io.netty:netty-all. Host verification in Netty is disabled by default. This can lead to MITM attack in which an attacker can forge valid SSL/TLS certificates for a different hostname in order to intercept traffic that doesn't intend for him. This is an issue because the certificate is not matched with the host.	WS-2020-0408
SwaggerUI supports displaying remote OpenAPI definitions through the ?url parameter. This enables robust demonstration capabilities on sites like petstore.swagger.io, editor.swagger.io, and similar sites, where users often want to see what their OpenAPI definitions would look like rendered. However, this functionality may pose a risk for users who host their own SwaggerUI instances. In particular, including remote OpenAPI definitions opens a vector for phishing attacks by abusing the trusted names/domains of self-hosted instances.	WS-2021-0461
In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561389; Issue ID: ALPS05561389.	WS-2021-0616
mruby is vulnerable to Heap-based Buffer Overflow.	WS-2022-0080
Command Injection in moment-timezone before 0.5.35.	WS-2022-0280
Cleartext Transmission of Sensitive Information in moment-timezone.	WS-2022-0284

Fixed Kernel Vulnerabilities

The following are the kernel vulnerabilities fixed in AGM 10.0.SP5:

- Missing Linux Kernel mitigations for 'MDS - Microarchitectural Data Sampling' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'Meltdown' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'Spectre variant 2' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'SRBDS - Special Register Buffer Data Sampling' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities

Known WhiteSource and CVE Issues in AGM 10.0 SP5

The following table lists known CESA issues in AGM 10.0 SP5:

Known Security Defects

Description	CESA #CESA #
CentOS: security advisory for bind	CESA-2021:3325
CentOS: security advisory for krb5-devel	CESA-2021:4788
CentOS: security advisory for glibc	CESA-2021:0348
CentOS: security advisory for bpftool	CESA-2022:5937, CESA-2022:5232
CentOS update for tcpdump centos7	CESA-2019:3976
CentOS: security advisory for rsync	CESA-2022:6170
CentOS: security advisory for open-vm-tools	CESA-2022:6381

The following table lists WhiteSource issues in AGM 10.0 SP5:

Known Security Defects

Description	WS #
Affected versions of JSON In Java are vulnerable to Denial of Service (DoS) when trying to initialize a JSONArray object and the input is [. This will cause the jvm to crash with StackOverflowError due to non-cyclical stack overflow. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	WS-2017-3805

The following table lists known Common Vulnerabilities and Exposures (CVEs) issues in AGM 10.0 SP5:

Known Security Defects

Description	CVE #
A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-3171
A flaw was discovered in Elasticsearch 7.17.0's upgrade assistant, in which upgrading from version 6.x to 7.x would disable the in-built protections on the security index, allowing authenticated users with "*" index permissions access to this index. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-23708
A cross-site-scripting (XSS) vulnerability was discovered in the Data Preview Pane (previously known as Index Pattern Preview Pane) which could allow arbitrary JavaScript to be executed in a victim's browser. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-23710
Scala 2.13.x before 2.13.9 has a Java deserialization chain in its JAR file. On its own, it cannot be exploited. There is only a risk in conjunction with Java object deserialization within an application. In such situations, it allows attackers to erase contents of arbitrary files, make network connections, or possibly run arbitrary code (specifically, Function0 functions) via a gadget chain. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-36944
In FasterXML jackson-databind before 2.14.0-rc1, resource exhaustion can occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled. Additional fix version in 2.13.4.1 and 2.12.17.1 **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-42003
In FasterXML jackson-databind before 2.13.4, resource exhaustion can occur because of a lack of a check in BeanDeserializer._deserializeFromArray to prevent use of deeply nested arrays. An application is vulnerable only with certain customized choices for deserialization. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-42004
Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-40149

Known Security Defects

Description	CVE #
Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by Out of memory. This effect may support a denial of service attack. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-40150
Apache Commons Text performs variable interpolation, allowing properties to be dynamically evaluated and expanded. The standard format for interpolation is "${prefix:name}", where "prefix" is used to locate an instance of org.apache.commons.text.lookup.StringLookup that performs the interpolation. Starting with version 1.5 and continuing through 1.9, the set of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote servers. These lookups are: - "script" - execute expressions using the JVM script execution engine (javax.script) - "dns" - resolve dns records - "url" - load values from urls, including from remote servers Applications using the interpolation defaults in the affected versions may be vulnerable to remote code execution or unintentional contact with remote servers if untrusted configuration values are used. Users are recommended to upgrade to Apache Commons Text 1.10.0, which disables the problematic interpolators by default. **Note:** *This vulnerability only applies to the optional catalog functionality of AGM.*	CVE-2022-42889

Known Kernel Vulnerabilities

The following are the known kernel vulnerabilities in AGM 10.0.SP5:

- Missing Linux Kernel mitigations for 'iTLB multihit' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'Spectre variant 2' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'MDS - Microarchitectural Data Sampling' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'Meltdown' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities
- Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities