
Actifio Global Manager (AGM) 9.0.x Release Notes

Updated Through Service Pack 9.0.7

Copyright, Trademarks, and other Legal Matter

Copyright © 2009 - 2020 Actifio, Inc. All rights reserved.

Actifio®, AnyIT®, Dedup Async®, OnVault®, Enterprise Data-as-a-Service®, FlashScan®, AppFlash DEVOPS Platform®, Copy Data Cloud®, and VDP® are registered trademarks of Actifio, Inc.

Actifio Sky™, Actifio One™, and Virtual Data Pipeline™ are trademarks of Actifio, Inc.

All other brands, product names, goods and/or services mentioned herein are trademarks or property of their respective owners.

Actifio, Inc., is a provider of data protection and availability products. Actifio's technology is used in products sold by the company and products and services sold and offered by its commercial partners. The current list of Actifio patents is available online at: <http://www.actifio.com/patents/>

Actifio believes the information in this publication is accurate as of its publication date. Actifio reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." ACTIFIO, INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This software and the associated documentation are proprietary and confidential to Actifio. Use, copying, and distribution of any Actifio software described in this publication requires an applicable software license. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

Actifio strives to produce quality documentation and welcomes your feedback. Please send comments and suggestions to docs@actifio.com.

Published May 12, 2020

Contents

Introduction	5
Before You Begin	5
Product Documentation.....	6
The ActifioNOW Customer Portal	7
Actifio Support and Service	7
AGM 9.0.7 Enhancements and Resolved Issues	9
New Features and Functionality in AGM 9.0.7	10
AGM web certificate is now complaint with the latest regulations	10
Reporting Manager Enhancements	10
Resolved Defects in AGM 9.0.7	11
AGM 9.0.5 Enhancements and Resolved Issues	15
New Features and Functionality in AGM 9.0.5	16
MySQL Database Management.....	16
Enhancements to the Logical Groups	16
SQL Server Always On Availability Group (AG) Enhancements	17
Improved Search Capability	17
Reporting Manager Enhancements	17
Resolved Defects in AGM 9.0.5	18
AGM 9.0.4 Enhancements and Resolved Issues	23
New Features and Functionality in AGM 9.0.4	24
Enhanced integration with IBM Db2 and SAP ASE (formerly Sybase ASE) database management.....	24
Integration with IBM Optim	24
Filter for Database Log Jobs	24
Reporting Manager Enhancement.....	24
Resolved Defects in AGM 9.0.4	25
AGM 9.0.3 Enhancements and Resolved Issues	29
New Features and Functionality in AGM 9.0.3	30
Replicating Data to Multiple Object Storage Pools	30
Policy Template Cloning.....	30
Organization Resource Membership.....	31
AGM-Report Manager Integration	31

Enhanced AGM Title Page	32
UI Enhancements.....	32
Library Updates	32
Resolved Defects in AGM 9.0.3	33
AGM 9.0.2 Enhancements and Resolved Issues	39
Upgrade Paths.....	39
New Features and Functionality in AGM 9.0.2	40
Report Manager (RM) Integration with Actifio Global Manager (AGM).....	40
Web Certificate Management	40
Changes to the Manage SLA Page	40
Adding Managed Applications to a Logical Group.....	40
Ability to List Applications where Manage Expiration is Disabled.....	40
Ability to Delete Multiple Unmanaged Applications	40
New Filter Options to Search by Template and Profile Name	41
Resolved Defects in AGM 9.0.2	42
AGM 9.0.1 Enhancements and Resolved Issues	45
Upgrade Paths.....	45
New Features and Functionality in AGM 9.0.1	46
SAP HANA Database Management	46
Manage Password Change	46
Enhanced Filter Preference	46
SQL Performance Improvements	46
Resolved Defects in AGM 9.0.1	47
AGM 9.0 Enhancements and Resolved Issues	51
New Features and Functionality in AGM 9.0	52
External Snapshot Pools with IBM Storwize/SVC and Pure FlashStorage.....	52
Expanded Cloud Mobility for Migration and Disaster Recovery	52
NFS datastore support with VMware (alternative to iSCSI)	53
NFS mount to Oracle RAC	53
Clone SQL Server to another server	53
Enhanced Cyber-Resiliency leveraging IBM Cloud Object Storage (COS) Retention Capabilities.....	53
Enhanced call-home functionality.....	53
Managed Data License (MDL) calculation for VSAN.....	54
Expanded support matrix	54
Usability and Performance Enhancements	54
VDP Features and Functions Not Supported in AGM 9.0	55
Limitations and Restrictions in AGM 9.0.....	56
Resolved Defects in AGM 9.0	58
Known Issues	67
Known Defects in AGM 9.0.7:	67

Security and Vulnerability Issues73

Security Fixes in AGM 9.0.7 73

CVEs Fixed in AGM 9.0.7 75

Known Security, WhiteSource and CVE Issues in AGM 9.0.7 84

Introduction

This document includes the release notes for Actifio Global Manager (AGM) 9.0 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:

- [AGM 9.0.7 Enhancements and Resolved Issues](#) on page 9
- [AGM 9.0.5 Enhancements and Resolved Issues](#) on page 15
- [AGM 9.0.4 Enhancements and Resolved Issues](#) on page 23
- [AGM 9.0.3 Enhancements and Resolved Issues](#) on page 29
- [AGM 9.0.2 Enhancements and Resolved Issues](#) on page 39
- [AGM 9.0.1 Enhancements and Resolved Issues](#) on page 45
- [AGM 9.0 Enhancements and Resolved Issues](#) on page 51
- [Known Issues](#) on page 67
- [Security and Vulnerability Issues](#) on page 73

Before You Begin

Upgrades to 9.0.x are supported from AGM 7.x and 8.x, with exceptions noted below. If you are running an older version of AGM then upgrade to the latest 8.1.x version first. You can also upgrade to 9.0.4 from all previous 9.0.x versions.

An AGM upgrade usually completes within thirty (30) minutes. The exact time depends on various factors, such as the number of appliances that AGM manages. If catalog or the reporting component is enabled, the upgrade may take a few minutes longer.

AGM 9.0.x can manage VDP appliances running version 7.1.x and up.

Exceptions:

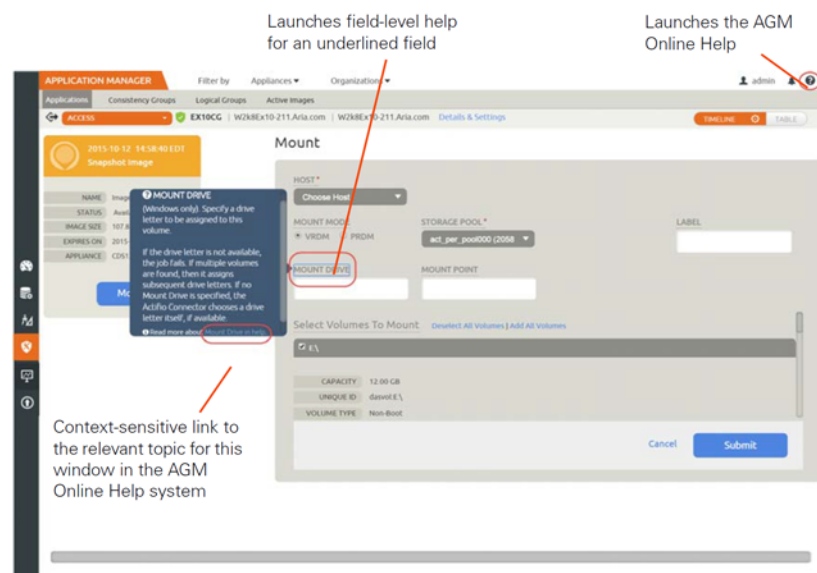
- If you are running AGM 8.1.6 or a later version, you will not be able to upgrade to AGM 9.0.1. This is because AGM 8.1.6 and later versions have certain functionality that is not available in AGM 9.0.1. When you plan to upgrade, consult with support and upgrade to a later version of AGM 9.0.x.
- VDP appliances running version 8.1.5 or later that use Catalog require AGM version 9.0.3 (with Hot Fixes) or later. Earlier versions of AGM are not compatible.

Product Documentation

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

Document	Description
<i>Installing and Upgrading Actifio Global Manager on VMware Server</i>	Provides information on how to deploy and install the AGM OVA file using the VMware vSphere Web Client.
<i>Installing and Upgrading Actifio Global Manager on Hyper-V Server</i>	Provides information on how to deploy and install the AGM OVA file using the Hyper-V Server.
<i>Deploying Actifio Global Manager in AWS</i>	Provides information on how to deploy AGM in AWS.
<i>Deploying Actifio Global Manager in Microsoft® Azure Cloud</i>	Provides information on how to deploy AGM in the Azure cloud.
<i>Deploying Actifio Global Manager in a Google Cloud Platform</i>	Provides information on how to deploy AGM in the Google Cloud Platform.
<i>Actifio Global Manager Release Notes</i>	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 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 provided you with a user name 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:
 - o **Product Documentation**—View the user documentation for your Actifio products and releases.
<https://actifio.force.com/c2/apex/C2ProductInformation>
 - o **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/

1 AGM 9.0.7 Enhancements and Resolved Issues

This section describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 9.0.7 release. It includes the following topics:

- [New Features and Functionality in AGM 9.0.7](#) on page 10
- [Resolved Defects in AGM 9.0.7](#) on page 11

For instructions on deploying AGM and Report Manager together, see the *AGM Installing and Upgrading* guide. To know more about the Report Manager (RM) component of AGM, refer to Reporting Manager enhancements, resolved and known issues sections.

New Features and Functionality in AGM 9.0.7

The following new features and enhancements have been introduced in AGM 9.0.7.

AGM web certificate is now compliant with the latest regulations

New AGM deployments now install a self-signed certificate in the AGM web server that complies with the latest security regulations and further tighten the security of AGM web server. (Bug 78284)

AGM also validates its web certificate on a daily basis. If the current web certificate is self-signed and it does not comply with the latest security regulations, or it is self-signed and will expire in the next seven days, AGM generates a new self-signed certificate and replaces the existing one. The web server on the AGM restarts and users are prompted to refresh their browsers due to the certificate change.

Note: *In prior releases, AGM provided the ability to replace the default self-signed certificates with a non-self-signed certificate that complies with the customer's security policies. If such a web certificate was installed, the daily web certificate validation described above will have no effect.*

Reporting Manager Enhancements

There are no new enhancements in this release.

Resolved Defects in AGM 9.0.7

The following list summarizes the defects resolved in AGM and Reporting Manager 9.0.7.

Resolved Defects

Issue	Fix	Tracking
AGM		
AGM was not remembering the “NFS Transport” option for a Host. When editing a Host that was previously saved with this setting, this option would show up as unselected.	AGM now shows this setting when editing a Host.	81636
When an appliance has two different values for “publicip” and “ipaddress” fields, AGM now uses the “publicip” as the cluster IP and uses this address to load the correct appliance configuration page.		81627
Standalone Non-RAC option was not being displayed for Oracle Consistency Group Liveclone configuration workflow.	This has been fixed and standalone non-RAC option is now available.	80997
For External Snapshot Pools (ESP), if a host did not exist on the external storage array, trying to enable/disable SLA was resulting in the following error “host could not connect to storage array”.	Issue has been fixed and you will no longer see the error message when enabling or disabling the SLA. You will only see the error message while creating or updating SLA if the host is unknown to the array or the host is not a VM.	80258
In the Manage expirations page, selecting “Shorten Retention By” did not automatically disable the “Extend Retention by” option.	The “Extend Retention by” option is disabled when the “Shorten Retention by” option is selected.	80061
A new Application and Details parameter for SAP HANA database, “Run Tenant Backups in Parallel”, has been introduced. When enabled, it allows the Connector to run the backup jobs of tenant databases in parallel rather than run one after the other.		80076
Clicking the “Appliance Configuration” option in AGM Domain Manager showed a blank page instead of the Appliance Configuration Setup page.	When the user clicks on the “Appliance Configuration” option, a new tab showing AGM Domain Manager opens up. It then redirects to the Appliance Configuration setup page.	80012
Editing a host with NFS staging disk resulted in the error “No more parsing elements”.	User will no longer see the error message.	79888
While adding a port, specifying a target with an extra IQN was resulting in AGM getting hanged.	Adding extra IQN now results in a pop-up message. User can review and click OK to close the message.	79676

Resolved Defects

Issue	Fix	Tracking
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 editing a host, AGM was unsuccessfully trying to reload the page.	The Edit Host page loads without any issue and the user can see a success message.	79217
During recovery of an OnVault image to a VMware target, the user could not select a Storage Pool, since it was an empty list. Moreover, running the recovery job resulted in an error "Invalid filter for numeric field id with value not a number".	User is able to select a value from Storage Pool drop-down option. In addition, the user can perform a successful recovery to a VMware target.	79201
When performing a mount as a new virtual machine, AGM user was not able to select the ESX and Datastore options for a vCenter as they were incorrectly grayed out.	User is able to select the ESX and Datastore options.	79116
During system recovery, AGM was unsuccessfully trying to load the datastore details even after the appliance was selected.	AGM correctly loads the datastore details when an appliance is selected.	78932
An issue involving the cursor display changing to a hand icon in the Add Applications page has been fixed.		78816
A new "Power Off After Recovery" toggle button has been added to the System State Recovery page. When this button is enabled, the target virtual machine is powered off after system state recovery.		78427
Catalog search results were incorrectly displayed in Internet Explorer.	Catalog search results 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.	Issue has been fixed and the AGM user is no longer forced to change password when updating email address or timezone.	78040
If all the appliances in AGM are in the stale state and an appliance is removed, AGM Dashboard was showing the error: <code>Java.lang.NumberFormatException: For input string: "clusterlist"</code>	Issue has been fixed.	77782
AGM was not showing the policies associated with an SLA Template created in an appliance.	All policies for an SLA Template created in an appliance are visible in AGM.	77567

Resolved Defects

Issue	Fix	Tracking
<p>When restoring an application, if the target host was a cluster host or cluster node, the restore page was freezing when trying to fetch the details.</p> <p>Since the default target was the source host, users would have seen this for all applications where the source host was a cluster host or cluster node, such as SQL AG.</p>	<p>This has been fixed and the Restore page no longer freezes.</p>	<p>76265</p>
<p>If the Mark Sensitive option was enabled for a workflow, it remained enabled by default even when the user tried to disable the option.</p>	<p>Issue has been fixed.</p>	<p>72163</p>
<p>The AGM user can now perform an application aware mount using the “Manage New Application” option when editing a workflow defined on a remote appliance. In previous versions, the action was resulting in an error message.</p>		<p>69085</p>

Reporting

<p>Schedule reports now show complete data even when the email schedule timezone is different from the Report Manager timezone.</p>	<p>80136</p>
---	--------------

2 AGM 9.0.5 Enhancements and Resolved Issues

This section describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 9.0.5 release. It includes the following topics:

- [New Features and Functionality in AGM 9.0.5](#) on page 16
- [Resolved Defects in AGM 9.0.5](#) on page 18

For instructions on deploying AGM and Report Manager together, see the *AGM Installing and Upgrading* guide. To know more about the Report Manager (RM) component of AGM, refer to Reporting Manager enhancements, resolved and known issues sections.

New Features and Functionality in AGM 9.0.5

The following new features and enhancements have been introduced in AGM 9.0.5.

MySQL Database Management

Actifio now supports data management of MySQL database applications. Databases are discovered automatically, transactions 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

- Automated discovery, backup/capture, and recovery of MySQL 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.

Enhancements to the Logical Groups

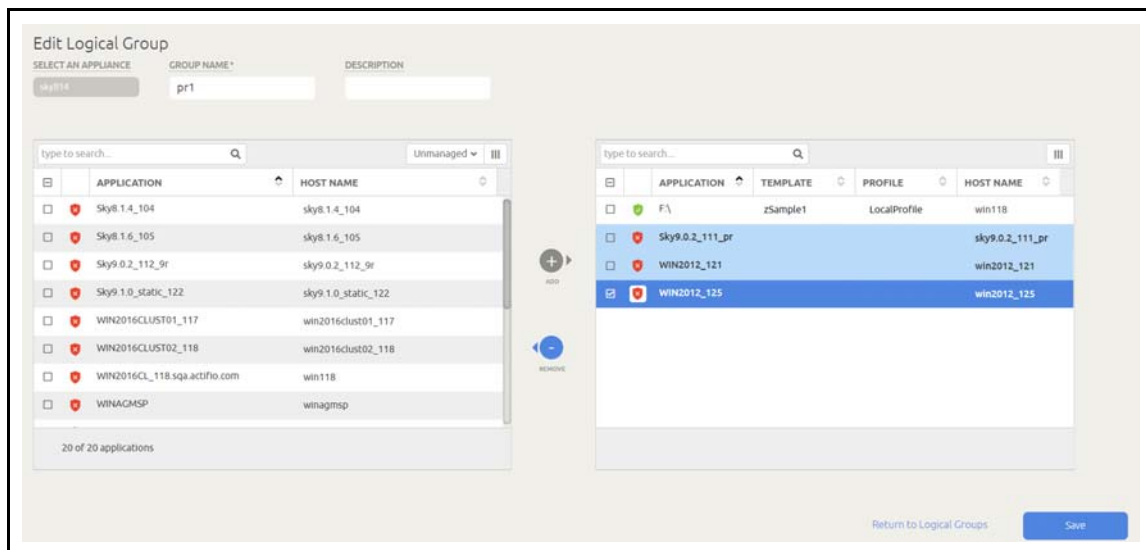
You can now create an empty Logical Group as a “placeholder” and add applications to the group later.



In addition, the Create Logical Group page has been updated with more user control including:

- easier filtering
- a search box on top left that queries applications
- ability to set columns as visible or hidden

In the Edit Logical Groups page, when adding applications to an existing group, the newly added applications are listed with a blue background.



SQL Server Always On Availability Group (AG) Enhancements

AGM now allows you to manage Microsoft SQL Server Always On Availability Groups (AG). Databases that belong to a SQL AG are automatically included for backups. Databases removed from an AG are automatically excluded from backup.

You can mount a SQL AG image as a virtual application to a new target, clone (copy) a captured SQL Server AG image to any physical or virtual host managed by your appliance, and restore a SQL AG either on-demand or as part of automated workflows.

Improved Search Capability

Implemented more efficient full text or keyword search to improve responsiveness of searches involving keywords. (Bug 76566).

Reporting Manager Enhancements

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:
 - o Application Growth
 - o Database Log Backup Summary
- Storage Resource Usage Summary report which was deprecated in 8.0.0. has been enhanced and added back under Utilization reports.
- System state recovery jobs are now included in the Recovery Job Details and Recovery Job Summary reports.
- The Restorable Images report now shows the mounted host name.
- Report Manager now supports storing the database partition on LVM to simplify growing the partition 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.

Resolved Defects in AGM 9.0.5

The following list summarizes the defects resolved in AGM and Reporting Manager 9.0.5.

Resolved Defects

Issue	Fix	Tracking
AGM		
Fixed a bug that could prevent Report Manager from starting properly.		78129
Concurrency handling capabilities have been enhanced. As a result, issues related to creating duplicate entries when a application is discovered from multiple appliances at the same time are now resolved.		76866
Dedup options section for dedup and remote dedup images was missing from the mount page.	Issue has been resolved.	77511
A new property, "Sybase Compression Level" is available for SAP ASE filesystem applications.		76803
The Local Auth column was incorrectly displaying 'No' for all users in the User Listing page regardless of actual setting.	This column has now been removed from the User Listing page.	76664
In the Edit screen for LiveClone with PrepMount workflow, when user switched from standalone instance to cluster instance the Map To All Cluster Nodes switch was being shown as 'Off'.	The issue has been fixed and the Map To All Cluster Nodes switch is now correctly showing as 'On'.	76273
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.	75919 75920
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. <i>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.</i>	75878

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 specified in minutes.	The interval is now correctly showing up as minutes if it had been saved as minutes.	75555
Listing applications for an Organization with a large Resource Membership resulted in a Server Request Failed error.	Issue has been fixed.	75112
Options to enter login credentials were presented even for Oracle database servers configured for OS authentication.	Login credentials are now requested only when the Oracle servers are configured for database authentication and when the database role is standby/secondary.	74856
The Clone action has now been removed for all custom application framework (CAF) applications.		74253
If a user tried to create a Logical Group containing a System state application without a boot volume, the Logical Group was still created even though group members could not be created due to the missing boot volume.	The issue has been fixed. In this situation, the Logical Group is no longer created.	74121
Display of remote snapshots associated with previous StreamSnaps took a long time to display (even a 15 minute delay had been observed).	Remote snapshots associated with previous StreamSnaps now display without any delay.	74000
In certain situations where AGM was managing a large number of appliances (over 100) and data replications were parallel, AGM was getting deadlocked in the UdsldGenerator due to massive concurrent database access.	The ID generation has been improved to prevent the deadlocks. In addition, the hibernate connection <code>pool max_size</code> has been updated from 25 to 50.	73956
When a scheduled Catalog job was started while a previous job was still running, the scheduler was getting stuck as the previous schedule was still running.	AGM Catalog feature allows only one cataloging job to run at a time. If any previous scheduled job is in progress, it will skip the current schedule.	73934
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.	73784

Resolved Defects

Issue	Fix	Tracking
Some queries for retrieving job history data have been implemented more efficiently so that they run faster and do not consume a large amount of temporary storage space in the database.		73742
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.	73665
The following error "For input string "2517693698" that AGM users could have seen in certain situations has been resolved.		73660
Issue with OutOfMemoryError exception in the Java heap after upgrading to AGM 9.0.4 has been resolved.		73417
Sorting behavior updated to change the past behavior that was introduced in Issue 69915: "Issue with indefinite wait for template listing in AGM SLA Architect has been fixed."		73163
After upgrading to AGM 9.0.4, users could no longer access the Pre and Post Scripts for workflows.	Issue has been fixed.	72708
When editing a Storage Array, the behavior of the "Clear" option after selecting some or all organizations has been corrected. Clicking the "Clear" button now correctly clears all selected organizations.		72176
The SLA Compliance settings for a Dedup Async policy is getting updated and reflected correctly.		72070
The Direct Mount and LiveClone workflow pages preserve the provisioning option values when a new target host is selected.		71855
An HTTP 404 error was shown when trying to reload the Appliance Configuration pages for an appliance running 9.0 SP1.	Issue has been fixed.	72010
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.		71782
The Move SLA functionality was not working as expected. It was not showing, for example, if the Move SLA was successful or if it failed. Also, "Moving SLA" display was simply changing from gray to red background on failure without error message.	The behavior has been corrected. On failure, the display changes from gray to red but with an error message. On success, background changes to green with success message.	71545

Resolved Defects

Issue	Fix	Tracking
Issue with uploading a Web Certificate to AGM when using Internet Explorer 11 has been fixed.		71377
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.	71369
When editing an OnDemand workflow, the field for Frequency is no longer displayed as it is not applicable to OnDemand workflows.		71130
When mounting an application, AGM was warning user to select the Mount Mode as pRDM even though the option is not appropriate.	The AGM UI prompts user to select the Mount Mode as pRDM only when appropriate.	71124
The Job list page of the System Monitor correctly filters the list view based on the keyword present in the URL.		70970
AGM timeout issues when deleting an SLA has been resolved.		70893
The page for managing Storage Arrays now permits individual storage arrays to be edited.		70810
A new hidden command (udtask restartcatalogdata) has been implemented for Admin users to clean up catalog related artifacts for a single application.		70692
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.		70346
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.		70093
An LDAP-authenticated user could not logout of AGM. An attempt to logout resulted in a spinner that never went away and the user stayed logged in.	The issue has been fixed and LDAP-authenticated users are able to logout of AGM now.	69438
Password restriction rules are now enforced for administrator users as well.		68175

Resolved Defects

Issue	Fix	Tracking
AGM users were able to edit organizations with same name and resources but with different IDs. Similarly, AGM users were able to edit multiple users and roles with the same name but with different IDs.	Issue has been fixed.	67369
Reporting		
The Resource Consumption by Application report now provides the Hide Headers & Footers option.		76008
Dedup Pool Consumption report uses case-sensitive sort by appliance name.		75069
Daily protection reports don't properly handle continuous policies.		74703
Running jobs and Backup Job Details reports include sub jobs.		73497
Storage Resource Usage Summary has inconsistent precision for percent.		72540
Not run jobs don't have job names in Daily Protection Table report.		72206
Job targets will not be populated from older appliances.		72003
Running Jobs report is missing filters.		72169
The Snapshot Consumption report now correctly handles snapshot pool renaming.		71570
Charts in the Managed Data Consumption Summary report can now be exported to PDF and other graphical formats.		69686
The Managed Data Consumption Summary report fixed incorrect calculations when calculating consumption by appliance and consumption by organization.		69684
Re-provision failed jobs are not under report failed jobs.		65620
Delete appliance takes a long time with no user feedback and shows an error message.		43485

3 AGM 9.0.4 Enhancements and Resolved Issues

This section describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 9.0.4 release. It includes the following topics:

- [New Features and Functionality in AGM 9.0.4](#) on page 24
- [Resolved Defects in AGM 9.0.4](#) on page 25

For instructions on deploying AGM and Report Manager together, see the *AGM Installing and Upgrading* guide. To know more about the Report Manager (RM) component of AGM, refer to Reporting Manager enhancements, resolved and known issues sections.

New Features and Functionality in AGM 9.0.4

The following new features and enhancements have been introduced in AGM 9.0.4.

Enhanced integration with IBM Db2 and SAP ASE (formerly Sybase ASE) database management

Actifio enhanced its out-of-the-box support for IBM Db2 and SAP ASE (formerly Sybase ASE). Databases are discovered automatically, transactions 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.

The following data capture methods and operating systems are supported:

- **Db2 and SAP ASE on Linux can be captured at the volume level** in an incremental-forever fashion with instant access and virtual clone creation for TDM. This leverages Linux LVM and Actifio's Changed Block Tracking capabilities and is the recommended alternative.
- For customers not using LVM or who cannot use volume level capture, Db2 and SAP ASE on Linux can alternatively be captured using full+incremental backup. This uses the databases' traditional "dump"-based backup, typically run as a weekly full and daily incrementals. Recovery involves reconstructing the incrementals on top of the latest full backup.
- **Db2 on AIX can be captured at the volume level** in an incremental-forever fashion with instant access and virtual clone creation for TDM. This leverages GPFS or JFS snapshots and synthesizes the incremental captures by running a full scan of the database to look for changed blocks. This alternative is recommended for TDM.
- For customers not using GPFS or JFS or who cannot use volume level capture, Db2 on AIX can alternatively be captured using full+incremental backup. This uses the databases' traditional "dump"-based backup, typically run as a weekly full and daily incrementals. Recovery involves reconstructing the incrementals on top of the latest full backup and therefore is not recommended for TDM.

Benefits

- Automated discovery, backup/capture, and recovery of Db2 and SAP ASE 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.

Integration with IBM Optim

Added integration in LiveClone workflows to run data masking using IBM Optim Data Privacy, leveraging a simplified setup procedure and without requiring any custom scripts.

Filter for Database Log Jobs

AGM can search for database log jobs in the System Monitor based on pre-defined filters. Two new filters options are available: Database and Logs and users can choose one or the other.

- When the Database filter is selected, all jobs that are of type DB or DB+Log are listed.
- When the Logs filter is selected, all jobs that are of type Log or DB+Log are listed.(67775)

Reporting Manager Enhancement

Daily Protection Reports support Dedup Async policy type.

Resolved Defects in AGM 9.0.4

The following list summarizes the defects resolved in AGM and Reporting Manager 9.0.4.

Resolved Defects

Issue	Fix	Tracking
AGM		
Issue with uploading a Web Certificate to AGM when using Internet Explorer 11 has been fixed.		71376
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.	71369
In the VM Onboarding Wizard, during resource profile selection, the profiles were displayed only in the mouse hover bubble.	Issue has been fixed.	70921
In certain situations where an application was found on multiple appliances, the 'Manage SLA' page for the application showed the 'Apply SLA...' button as active even though the application belonged to a managed Logical Group.	The 'Apply SLA...' option is grayed out in this situation.	70627
In the Run Workflow page, the Submit button did not respond when user selected and configured the Refresh Existing Virtual Application option.	The Submit button now responds when user selects the Refresh Existing Virtual Application option.	70590
When adding applications using an IP address, the loading icon did not display and the response time was slow.	User will now see the loading icon when adding applications using IP address. The response time for adding an application has also been improved.	70533
In the Change password dialog, the Save option was active even when the new password was less than six characters.	The 'Confirm password' property and the 'Save' button are disabled if the new password is less than six characters.	70455
AGM Workflow page displayed Manage New Application toggle button as off even though the child database was managed.	Issue has been fixed.	70371
Adding storage array failed with error "Failed to return newly-created array." even though the Test Connection was successful.	Storage array can be created without any error.	70296

Resolved Defects

Issue	Fix	Tracking
The Run Once Per Window option in the Create or Edit policy dialog was incorrectly accepting zero (0), negative, and non-numeric values.	User will see an error message if s/he provides zero (0), negative, and non-numeric values.	69921
Issue with indefinite wait for template listing in AGM SLA Architect has been fixed.		69915
When creating a Streamsnap policy, the time specified to start the first job was not being saved.	This issue has been fixed.	69883
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 not accept zero (0) or non numeric value. If the user clears the property text box, it will retain the previously assigned value.	69844
The Run Workflow and Edit Workflow pages no longer freeze up when an incorrect or invalid host Id is provided. Instead, an appropriate error message is displayed.		69784
For new workflows associated with application type "LVM Volume," the mount location and mount action are now being correctly sent to the AGM server when the user selects Run Now.		69696
Issue with LDAP settings changing when a user switched from local to LDAP authentication is fixed.		69486
Alignment issue for the Auto Create User option in the Create LDAP authentication page (of Domain Manager > Authentication is fixed.		69484
AGM supports multiple IP addresses when performing a restore operation over NFS. It recognizes alternative IPs associated with a host when performing restore.		69356
The Consistency Group Edit page freezes when the user tried to rename the Consistency Group with the existing name.	User will see an error message if she renames the Consistency Group with the existing name.	67536
In the Run Workflow page, selecting the "Refresh an Existing Virtual Application" option, would not show the Host list.	The host list is now available.	67443
AGM was hanging when user selected the Cancel option immediately after selecting a host in step 1 of the VM Onboarding Wizard.	The wizard does not hang when user selects a host and user is able to go to the next page.	59499
Amazon VPC ID was incorrectly described as Network ID in the Recover System page.	Issue has been fixed.	45590

Resolved Defects

Issue	Fix	Tracking
Reporting		
Bandwidth Utilization History reports all 0s.		71196
Reporting data sync could fail with VDP appliances that used an OnVault enforced retention policy.		70995
Opening xlsx output of Backup Job Details reports "We found a problem with some content".		68836
Upgrade failed as /tmp has huge number of file.buff.os.8343521946*****.tmp files.		68756

4 AGM 9.0.3 Enhancements and Resolved Issues

This section describes the new features and enhancements, as well as resolved defects in the Actifio Global Manager (AGM) 9.0.3 release. It includes the following topics:

- [New Features and Functionality in AGM 9.0.3](#) on page 30
- [Resolved Defects in AGM 9.0.3](#) on page 33

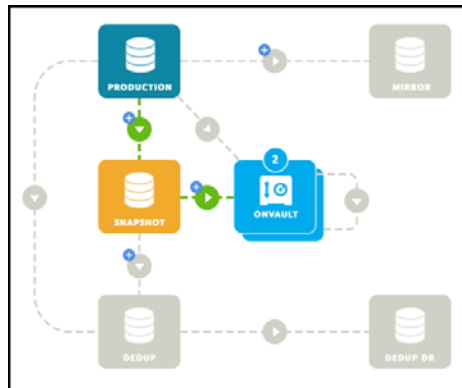
VDP appliances running version 8.1.5 or later that use Catalog require AGM version 9.0.3 (with Hot Fixes) or later. Earlier versions of AGM are not compatible.

New Features and Functionality in AGM 9.0.3

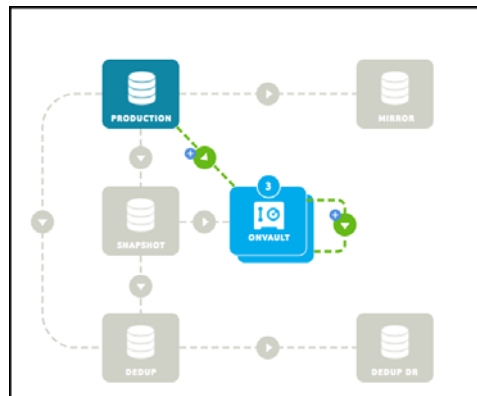
The following new features and enhancements have been introduced in AGM 9.0.3.

Replicating Data to Multiple Object Storage Pools

AGM users can replicate data captured in a Snapshot Pool to one or more OnVault Storage Pools. When two or more Snapshot to OnVault policies with different target pools are defined for a template, the OnVault icon shows a shadow to indicate there are multiple target pools for this template. In the image below, for example, there are two different Snapshot to OnVault policies defined with different target pools.



Users can also replicate data from a Direct to OnVault image to another OnVault pool as shown below.



Replicating data to multiple object storage pools allow:

- Data resiliency across multiple geographic locations using various clouds and/or vendors.
- Data to be used for disaster recovery, as well as for test/development environments in different geographic locations.
- Jobs to replicate to multiple targets that run concurrently.

Policy Template Cloning

The template cloning capability in AGM allows users to easily create a similar template from an existing template. When cloning multiple templates, a clone is created for each of the selected templates. The cloned template will get listed as: Copy of <original_template name>_<year>_<month>_<date>_<hour>_<minute>_<second>.

Organization Resource Membership

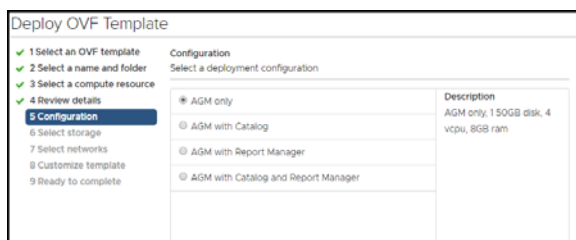
The “Organization Resource Membership” section in the create and edit organization pages in the AGM UI allows users to assign various resources to an organization. The same resource can be assigned to one or more organizations. The following resource types can be assigned to an organization:

- **Templates:** Collections of policies. A policy defines how the backup data is managed. For example, it defines the type of the backup operation (snapshot, deduplication, replication, and so on), frequency of the backup operation and life-time of the backed up data.
- **Profiles:** Specifies the storage media for the backed up data.
- **Users:** AGM users of any level.
- **Hosts:** Data resources that are protected by AGM. Hosts can be physical servers or hypervisors.
- **Applications:** Generic term for data resources (including Consistency Groups) to be protected by an appliance.
- **Storage Pools:** Storage resources.
- **Storage Arrays:** External storage arrays like IBM Storwize and Pure storage.
- **Logical Groups:** Logical grouping of applications from one or more hosts for ease of management.

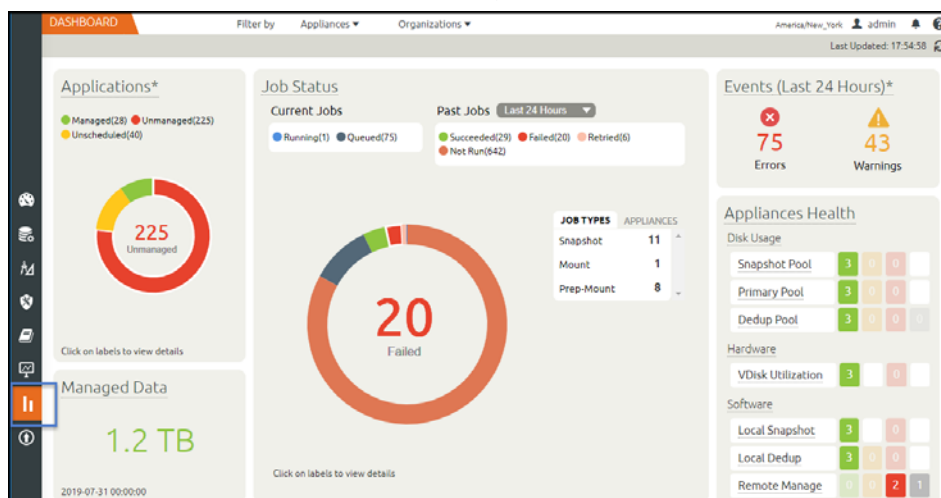
AGM-Report Manager Integration

This release adds the following enhancements to the AGM-Report Manager integration:

- **AGM-RM installation changes:** Users have the option to deploy AGM with and without Report Manager. This is in addition to the options of deploying AGM with or without Catalog. The following image is from deploying AGM in a vSphere client.

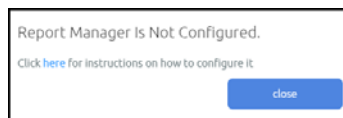


- **AGM UI changes:** Users can access RM from the AGM UI by clicking on the RM service icon on the left panel.



If the Report Manager is configured for use, a new page will open showing the Report Manager login page. Use your AGM username and password to login to Report Manager.

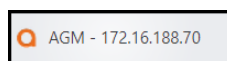
In case the Report Manager is not configured, you will see the following message.



You can click on the link in the message to go to the Online Help for instructions on how to add resources to enable Report Manager.

Enhanced AGM Title Page

The browser tab now shows the product name AGM along with the IP address or the host name of the AGM server as specified in the URL. This allows the user to easily identify an AGM server when there are multiple AGM servers in their enterprise. (Bug 64460)



UI Enhancements

Search terms are now persistent across browser sessions and the search bar and grids automatically filter results based on these persistent search terms. This behavior applies to all grids including Jobs, Events, Applications, Active Images, Workflows, Hosts, Storage Pools, and Storage Arrays. (Bug 67556).

Library Updates

The following libraries were updated to include the latest security fixes:

- Mustache (fixed CVE-2015-8862)

Resolved Defects in AGM 9.0.3

The following list summarizes the defects resolved in AGM 9.0.3.

Resolved Defects

Issue	Fix	Tracking
Fixed a compatibility issue with VDP appliances that use Catalog running version 8.1.5 and above.		70328
AGM supports multiple Internet Protocol (IP) addresses when performing a restore operation over NFS. It recognizes alternative IPs associated with a host when performing restore.		69143
User was unable to perform any clone operation even with Backup Manage, Clone Manage, Mount Manage, and Storage Manage access control rights.	Issue has been corrected and an AGM user with the correct access control rights is able to perform clone operations.	68916
When cloning a Consistency Group with SQL databases, the Submit button got enabled before any selections were made.	Issue has been fixed and the Submit option is enabled only after the user has provided the information necessary for cloning.	68617
An alignment issue where clicking the AGM left panel shifted the Move SLA dialog towards the bottom of the page has been fixed.		68426
Alignment issue where the "Select Export Format" was not rendered properly has been fixed.		68254
The Run Now operation on a LiveClone Workflow configured for a SQL application, failed to pass the password value.	Issue has been fixed and the password gets correctly picked up during the Run Now operation.	68217
During a remount operation, by default, the source host now gets pre-populated with the unmounted host.		68181
A performance issue has been fixed with loading the details of a DAR image from the Application Manager's Access page for LVM and non-LVM applications.		68121
Application aware mount options for Oracle applications in a Consistency Group are now available.		68100
Fixed an issue that made a System State application incorrectly show the excluded Filesystems as still included, specifically when the System State application was replicated with Dedup Async or StreamSnap.		68081
In the System Monitor, a performance issue related to querying and rendering of enormous job histories (greater than 1 million jobs) has been fixed.		67950
AGM was continuously loading the System State recovery page when a user tried to change the ESX server details to None.	The System State recovery page loads quickly after a user updates the ESX server details to None.	67869

Resolved Defects

Issue	Fix	Tracking
If Report Manager is configured, and a user deletes an appliance from AGM, the following message is now shown: "The appliance is still included in reporting for historical data"		67818
When the global filter for Organization is enabled, SLA filters were displaying very sluggishly in the Application Manager.	The performance issue with display of SLA filters has been fixed.	67795
The AGM user now sees the Appliance list page after canceling out of the Add Appliance page. In previous releases, after canceling out of the Add Appliance page, the user was redirected back to the same page.		67787
When importing an OnVault image, the drop-downs to select source pool and target appliance were disabled and it was not possible to make selections.	This defect has been fixed, and the drop-down lists are populated correctly and enabled when importing OnVault image.	67684
You can now map a new LDAP Group with roles and organizations.		67666
You can now select the source, as well as destination pools when importing an OnVault image.		67650
The Description column of the Applications list page was empty.	The Description column now shows notes about the application.	67648
Users were getting an error applying an SLA to manage a VM application when the selected Resource Profile's data storage location was an External Snapshot Pool. This was because a connection to the external storage array could not be established.	Users can now successfully apply an SLA to manage a VM when the selected Resource Profile's data storage location is an External Snapshot Pool.	67620
Improvements in performance and significant reduction in delays and gridlocks when a large number of applications, for example SQL Instances with over two thousand (2000) applications, are replicated.		67562
Consistency Group Management functionality has been enhanced to support applications discovered from multiple appliances.		67409
AGM is now capable of saving Oracle workflows with SLT and SLP for newly provisioned App-aware mounts.		67325
Fixed a defect where adding an organization to multiple selected templates in SLA Architect was failing to add the organization.		67307
When an IBM Storwize array is added, an Add External Snapshot Pool option is now displayed under AGM -> Domain Manager -> Storage Pools. Previously this option was not shown.		67293
Resolved an issue that prevented file-catalog searches from working on some newly installed appliances using AGM.		67216

Resolved Defects

Issue	Fix	Tracking
Resolved an issue that prevented the dashboard from properly rendering for some users with restricted permissions.		67130
New settings for calculating AGM replication interval broke existing interpretation of properties replicate.schedule.interval and replicate.schedule.ticks, thus causing user-specified intervals to work incorrectly.	This has been fixed and backward compatibility logic has been put in place so that user-specified settings are correctly interpreted.	67118
Users can now create new Consistency Groups and update existing Consistency Groups with member applications that are discovered on multiple appliances.		67048
When the volume information of a component was not available, AGM did not display the other available information about the appliance (for example, Name and Type).	AGM now displays all available information about an appliance even when the volume information is not available.	66987
An issue where the Secure flag was not getting explicitly set for a cookie has been fixed.		66979
Fixed a security issue that was potentially allowing upload of malicious code into an appliance, that could then be executed to bypass rbash security.		66966
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'.		66933
In the Application Manager, under "Unmanaged SQL Instance > Manage SLA > Database Inclusion Rule", when a single database was selected under that inclusion rule and subsequently if that database was individually protected, then the Manage Workflows view could not be displayed.	This defect has been fixed, and under the stated condition, clicking the Manage Workflow menu item correctly brings up the Manage Workflows view.	66923
In the AGM severity filter selection, the filters were being displayed in alphabetical order (error, info, warning) instead of severity order.	The filters are now being displayed in severity order (info, warning, error).	66747
Two new parameters "sqlbuffercount" and "sqlmaxtransfersize", that were previously added to VDP Desktop version 9.0 SP2, have now been made available in AGM.		66645
Under Application Manager's Application list page, selecting the image type filter as 'dedup' caused applications with 'remote-dedup' image type to get displayed as well.	This has been fixed and the filter now correctly lists only those applications containing the selected image type.	66603
The "Manage Expirations" option did not work for any backup image from a restore operations page.	The "Manage Expirations" option is now working from all types of restore pages.	66600

Resolved Defects

Issue	Fix	Tracking
The AGM UI was hanging when a user attempted to delete a host that had mounted images.	The issue has been addressed and the user is shown an error message stating that there are mounted images associated with the host.	66558
When creating an SLP, AGM now validates that the vault pool specified in the operation actually belongs to the target appliance.		66542
The AGM user interface no longer displays the End User License Agreement on every login once the "SHOW AGAIN" option is turned off at the bottom of the license agreement.		66495
Upgrade from AGM 8.1.6 has been fixed and the new AGM service starts up correctly after the upgrade.		66481
In Application Manager's Applications list page, when the user selected the Manage SLA option to protect an unmanaged application, the Apply button remained disabled. As a result, the user was not permitted to save any changes to the template.	Now when a user modifies a template, the Apply button is enabled, allowing the user to the changes made to the template.	66420
In the SLA Architect, when a new SLA template is created with a snapshot policy, the "SLA Compliance" settings are kept disabled till the new template is saved. This prevents misleading errors caused by attempts to access SLA compliance settings on a Snapshot policy that has not yet been created.		66377
In the Manage Workflow page, the option to select all hosts now honors the search criteria specified in the search filter for hosts. Previously, clicking the check box to select all hosts selected even those that did not meet the search criteria.		66300
In the Consistency Group creation page, a spinner is displayed while the host list for the selected appliance is still refreshing. This prevents a user from changing the appliance selection until all hosts have been refreshed, thus avoiding inconsistent host lists.		66073
On the Create Workflow page, the option to select all databases now works correctly; it selects all available databases in the list.		66068
During SLA creation, user-specified application level options for the SLA were getting ignored when the SLA was activated for the first time. This was caused by a defect in the order in which SLAs were saved and activated.	The sequencing has been corrected and SLA options are now correctly recognized and activated when an SLA is created.	65487
The AGM user can update a resource profile by selecting the option "None" for the OnVault and Remote appliance properties. In prior releases, a resource profile configured to use an OnVault pool and/or a remote appliance, did not allow the user to select the option "None".		64194

Resolved Defects

Issue	Fix	Tracking
AGM now validates that workflows with RAC nodes must have the nodes specified as IP addresses, not as node names.		62166
As a result of performance improvements, when applying rule changes to SQL instances, AGM no longer displays the “Updating rules” screen that previously prevented users from performing other operations while the updates were in progress.		61993
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.	61141
The following properties: “Application ID” “Application Type,” and “Job Name” are now available in the Events > View Details page of the AGM UI.		40569

5 AGM 9.0.2 Enhancements and Resolved Issues

This section describes the new features and enhancements as well as resolved defects in the Actifio Global Manager (AGM) 9.0.2 release. It includes the following topics:

- [New Features and Functionality in AGM 9.0.2](#) on page 40
- [Resolved Defects in AGM 9.0.2](#) on page 42

Upgrade Paths

VDP appliances running version 8.1.5 or later that use Catalog require AGM version 9.0.3 (with Hot Fixes) or later. Earlier versions of AGM are not compatible.

New Features and Functionality in AGM 9.0.2

AGM 9.0.2 contains new features as well as usability and security enhancements.

Report Manager (RM) Integration with Actifio Global Manager (AGM)

Report Manager (RM) can now be installed as part of AGM and run in the same virtual machine (additional memory and CPU are required). This integration simplifies deployment and streamlines ongoing management. When deployed in this integrated configuration:

- User authentication to RM is done via AGM, instead of one of the appliances. This means that any AGM user can log in to RM.
- Organization membership information is pulled from AGM.
- All appliances managed by AGM are automatically added to RM. Additional appliances can be manually added to RM.
- All upgrades are done through the AGM UI and include upgrades to both AGM and RM components.
- The AGM version is always listed, even from the RM Help > About dialog.

For instructions on deploying AGM and RM together, see the *AGM Installing and Upgrading* document. For more information on new capabilities of RM 9.0 see the *Report Manager 9.0 Release Notes*.

Web Certificate Management

AGM users with administrator role can:

- Upload PKCS #12 certificate to replace the existing TLS certificate
- Re-generate a new self-signed TLS web certificate

This is useful for customers who need to comply with their security model.

Changes to the Manage SLA Page

The Manage SLA page has the following enhancements among other changes:

- The 'Apply SLA' option has been updated to 'Apply SLA...' to indicate that further actions are needed from the user in order to apply the SLA to unmanaged applications and consistency groups.
- Within the 'Apply SLA' dialog, the Save option has been renamed to 'Apply SLA'. This option is disabled till all the required properties (marked in red asterisk) are filled in.

Adding Managed Applications to a Logical Group

Users can now add managed applications to a Logical Group, with the following conditions:

- Selected application(s) should belong to the same appliance and should not be an existing member of a Logical Group.
- Selected application(s) must be managed by the same SLA (template and profile) as the Logical Group.

Ability to List Applications where Manage Expiration is Disabled

A new filter option 'Disabled Only' has been added to list applications where the 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" for applications that have enabled image expiration, and show the value "No" for applications that have disabled expirations. (Bug 64272).

Ability to Delete Multiple Unmanaged Applications

AGM users can delete multiple unmanaged applications and/or VMs from the Application Manager list view.

New Filter Options to Search by Template and Profile Name

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.

Resolved Defects in AGM 9.0.2

The following list summarizes the defects resolved in AGM 9.0.2.

Resolved Defects

Issue	Fix	Tracking
User was unable to manage expiration of an image from the Restore page.	The Manage expirations option is working correctly during restore operation.	66565
When a user wanted to create a template Snapshot policy with replication type of 'Stream Snap', an attempt to bring up 'SLA compliance' settings resulted in a blank screen.	Trying to define 'SLA compliance' before the template for Snapshot policy is not allowed. Attempts to bring up the 'SLA compliance' setting prior to saving template now results in an error display: An error occurred while trying to edit SLA compliance thresholds. You can continue editing other parts of this policy.	66359
A typo in Catalog's Select Data Capture view has been fixed.		66356
During System State recovery, some required fields for VM recovery were grayed out and could not be filled.	The required fields for VM recovery are now available.	66323
AGM user was unable to navigate to other pages within the AGM UI after enabling database log backup for more than one policy in a template.	Issue has been fixed and user can go to Create and Edit policy pages and access other AGM services.	66164
Search capability in the Add Application view was not working.	Users can search by entering text in the search dialog box and then filter the results by host, IP address, or friendly path.	66142
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.	65951
The SQL Server instance name was not showing in the Run Now page when the user selected a different host. This was because, the user was not able to see the SQL Server instance associated with that host.	Issue has been fixed and the instance name is correctly getting populated.	65887
VM cluster was not showing in AGM.	VM cluster is now visible.	65526
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.		65502

Resolved Defects

Issue	Fix	Tracking
During VM discovery, user had to wait a very long time (upwards of eight minutes) before she could navigate to the next page of the wizard.	User is no longer experiencing delay when discovering VMs.	65242
Provisioning a template triggered Null Pointer Exception when the target appliance was in stale mode with no version information.	Provisioning a template is now successful even if the target appliance is in stale mode and has no version information.	65136
SLA compliance was getting enabled for appliances belonging to unsupported versions.	Appliance version checks have been implemented. SLA compliance is enabled only when appliance version is 9.0+ / 8.1.2+ / 8.0.9+ and when SLA compliance is enabled on any of the appliance.	65047
In the create workflow page, the 'Name of the Consistency group' option was not showing even after the user had selected one or more databases.	AGM UI is now displaying the 'Name of Consistency group' option when one or more databases are selected.	65012
After upgrading AGM, the Catalog menu in the AGM UI not available to the user, even though the catalog service was running and indexing images.	The Catalog menu in the AGM UI is available after upgrading AGM.	64944
The pRDM and vRDM options for edit workflow page was missing for workflows that was created in a version of AGM prior to 8.1.3.	The pRDM and vRDM options have been added to provide backward compatibility for workflows created in versions of AGM earlier than 8.1.3.	64816
When configuring a VMware vSAN policy, if you had set the "Primary level of failures to tolerate" option to greater than zero (0), VDP was over reporting consumed MDL.	Issue has been fixed and the MDL for vSAN volumes is now correct.	61093
SystemState Recovery page was listing Performance Pool title instead of Snapshot Pool.	SystemState Recovery page lists Snapshot Pool.	58259

6 AGM 9.0.1 Enhancements and Resolved Issues

This section describes the new features and enhancements as well as resolved defects in the Actifio Global Manager (AGM) 9.0.1 release. It includes the following topics:

- [New Features and Functionality in AGM 9.0.1](#) on page 46
- [Resolved Defects in AGM 9.0.1](#) on page 47

Note: *If you are running AGM 8.1.6 or a later version, you will not be able to upgrade to AGM 9.0.1. This is because AGM 8.1.6 and later versions have certain functionality that is not available in AGM 9.0.1. When you plan to upgrade, consult with support and upgrade to a later version of AGM 9.0.x.*

Upgrade Paths

If you are running AGM 8.1.6 or a later version, you will not be able to upgrade to AGM 9.0.1. This is because AGM 8.1.6 and later versions have certain functionality that is not available in AGM 9.0.1. When you plan to upgrade, consult with support and upgrade to a later version of AGM 9.0.x.

Also, VDP appliances running version 8.1.5 or later that use Catalog require AGM version 9.0.3 (with Hot Fixes) or later. Earlier versions of AGM are not compatible.

New Features and Functionality in AGM 9.0.1

AGM 9.0.1 contains new features as well as usability and security enhancements.

SAP HANA Database Management

Actifio now supports data management of SAP HANA database applications. You can now protect SAP HANA databases using:

- HANA storage snapshot APIs while leveraging VDP Linux CBT and LVM snapshot to realize incremental forever backup.
- HANA file-based API to realize traditional backups with option to configure weekly full and daily incremental backups.
- Option to back up HANA logs.

Benefits

- Automated discovery, backup, and recovery of HANA databases.
- Log roll forward option to recover HANA database to any point in time.
- Automated deployment of virtual copies (application aware mount) for TDM use cases.
- Supports a broad range of SAP HANA configurations:
 - o Single container system (HANA 1.0)
 - o MDC: Multiple container systems (HANA 2.0) with one tenant database
 - o MDC: Multiple container systems (HANA 2.0) with more than one tenant database
 - o Scale-out MDC: Multiple container systems (HANA 2.0) with one or more tenant database
 - o Scale-out MDC: Local HA (N active hosts + 1 or more standby nodes)

Manage Password Change

AGM now allows users to change their own password at any time. In addition, for new AGM deployments, the admin is prompted to change the password when logging in for the first time.

Enhanced Filter Preference

A user's filters of type text, list, or date are remembered across different AGM sessions, even if the user switches browsers or connects to AGM from a different machine.

SQL Performance Improvements

UI performance improvements when dealing with SQL Server Instances with thousands of databases.

Resolved Defects in AGM 9.0.1

The following list summarizes the defects resolved in AGM 9.0.1.

Resolved Defects

Issue	Fix	Tracking
The Connectivity status of an appliance added to AGM from the Domain Manager tab was incorrect.	The connectivity status is reported correctly.	64739
Text alignment issues in the Configure LDAP page have been corrected.		64479
Oracle ASM switch operations failed when the target host was a VM.	AGM automatically uses physical RDM when the target host is a VM.	64325
After detecting and displaying the error that an upgrade file is older than the current installed version of AGM, the process still proceeded to the upgrade screen when the user clicked Okay.	The process no longer takes the user to the upgrade screen when the user clicks Okay on the error message popup.	64036
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.	63805
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".		63725, 62448
New access permission, "Catalog Access" is now available. It allows non-administrator AGM users to access and use Catalog functionality.		63463
Removed deprecated DSA keys.		63419
Login to AGM was failing when a role owned by a non-admin user got deleted.	Issue has been fixed by assigning the BASIC role to the non-admin user in this scenario.	63184
AGM search now has an option for exact match to find specific LDAP groups quickly.		63079
In certain situations, deleting a workflow from AGM was failing with a read timeout error message.	The read timeout when deleting workflows has been increased and the AGM user will no longer see the read timeout error message.	62933
The Organizations panel in the LDAP Group Mapping page was showing an empty list when more than one hundred (100) organizations defined in AGM.	The Organization panel lists all organizations.	62863

Resolved Defects

Issue	Fix	Tracking
AGM user without access to source host could not run on-demand workflows.	Issue has been fixed.	62681
Removed deprecated SSH key exchange algorithm diffie-hellman-group1-sha1.		62621
Unable to submit an application aware mount job of Oracle child database for 8.1.x and older appliances as the child database was missing application metadata.	User can now submit application aware mount job of Oracle child database for 8.1.x and older appliances.	62501
When adding a host for the first time from Domain Manager in AGM, if there were more than eleven (11) appliances available to add, then some of them may 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 lists all available appliances.	62364
Remounting an image with a custom letter drive that was originally mounted without any customization results in error: "Mount is unsuccessful due to partial mount only allowed on original image"	User can successfully remount an image with a custom letter drive.	62240
AGM now displays the correct region code when AGM is loaded for the first time for GCP targets.		62191
AGM now recognizes when a private IP address is not required for recovery on AWS, and permits recovery on AWS without forcing users to specify a private IP address.		62189
Issue with the missing OnVault Pool column in the SLA Architect's, Profile page has been fixed.		62120
User was unable to perform 'Failback' operation from the 'Table view' page of the Application Manager.	'Failback' operation is successful run from the 'Table view' page.	62054
Selecting job number in the System Monitor was not refreshing the job details.	Job details gets refreshed.	62038
The Dashboard page may show a mismatch of appliance count in Desktop and AGM. This is because the filters in Desktop and AGM are different.		61951

Resolved Defects

Issue	Fix	Tracking
For SQL applications discovered from VM's, if the user selected EnableMountToVirtualSqlCluster parameter to False, the WorkFlow configuration page did not show the Mark Dependent option when vRDM is selected.	Issue has been fixed for SQL and FileSystem applications.	61925
On the Manage Membership for SQL Instance page, with Show Selected check box turned on, when some database instances are first selected for a database inclusion rule and subsequently all database instances are de-selected, then none of the database instances showed up as selected even though the count of selections was correct.	Issue has been resolved. When no database instance is selected, then all database instances are displayed when Check Selected check box is turned on. The set of databases displayed is in sync with the selection count displayed.	61498
Non administrator AGM users without sufficient rights were seeing a confusing and empty error message when logging into AGM.	Non administrator users without sufficient rights now see the following error message: User does not have sufficient rights to get system information.	61114
In the VM Onboarding Wizard pages, if a user accidentally double-clicked the Cancel option, the UI was not presenting the "Before You Cancel" dialog with prompt to stay in the same page or exit to Application Manager.	If the user accidentally doubles clicks the Cancel button instead of single click, the user is now presented an option to cancel and go back to the Onboarding page.	58698
The Event Id information was missing in the job details page.	The Event Id details are now available.	58213
Attempting to remove a policy from a template in AGM resulted in a 10053 error - Provisioning operation not performed, waiting for cluster lock.	Templates can now be deleted in AGM.	50359
For Host types that are hosting VMs (hypervisor hosts), AGM now displays options to "Add Virtual Machines", which then provides a wizard to discover VMs. Previously, it displayed options to discover applications, which is not applicable to hosting VMs. The fix applies to vCenter as well as Standalone ESX.		50033

7 AGM 9.0 Enhancements and Resolved Issues

This section describes the new features and enhancements, limitations and restrictions, as well as resolved defects in the Actifio Global Manager (AGM) 9.0 release. It includes the following topics:

- [New Features and Functionality in AGM 9.0](#) on page 52
- [VDP Features and Functions Not Supported in AGM 9.0](#) on page 55
- [Limitations and Restrictions in AGM 9.0](#) on page 56
- [Resolved Defects in AGM 9.0](#) on page 58

Note: The features available in the Domain Manager for appliance setup will vary according to your appliance version. The features described in this release note and the AGM Online Help reflect the latest release of the appliance. Version specific features are identified as such.

For a comprehensive list of known defects in AGM 9.x, see [Known Issues](#) on page 67. For a list of CVE fixes, see [Security and Vulnerability Issues](#) on page 73.

Note: AGM 9.0.x can manage VDP appliances running version 7.1.x and up. VDP appliances running version 8.1.5 or later that use Catalog require AGM version 9.0.3 (with Hot Fixes) or later. Earlier versions of AGM are not compatible.

New Features and Functionality in AGM 9.0

The following new features and enhancements have been introduced in AGM 9.0

External Snapshot Pools with IBM Storwize/SVC and Pure FlashStorage

Actifio has extended its Virtual Data Pipeline (VDP) to manage and use 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.

Application data can be captured in an incremental-only fashion by snapping the production LUNs in-place (using them as the base), or they can capture data in a full+incremental fashion (aka out-of-band) into an external snapshot pool in a different array, to create a full copy of the data set first and then copy incremental changes.

While capture methods differ, array snapshots are leveraged in both cases and can be mounted directly to hosts, thereby leveraging the arrays connectivity (FC or iSCSI), high-availability, and performance.

Once data is captured into the external snapshot pool, it can still flow into the Virtual Data Pipeline in an incremental-forever manner to leverage VDP capabilities, including OnVault, dedup, remote dedup, StreamSnap, and Dedup-Async replication.

Highlights

- Better performance on mounted images. Activity on virtual clones does not go through the VDP appliance but rather directly between the host and storage array. This is especially important in test/development environments.
- Better performance and recovery time objective (RTO) for disaster recovery (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 VDP appliance).
- Incremental-Only capture for applications 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.
- Fibre Channel host connectivity with Sky appliance (Sky to array connection is iSCSI).
- Better scalability of VDP infrastructure, where fewer appliance will be needed.
- Wider support matrix - interoperability according to the array's connectivity.

Expanded Cloud Mobility for Migration and Disaster Recovery

When using cloud mobility to recover physical and virtual systems into a cloud environment (AWS, Google Cloud Platform, Microsoft Azure), users can request to copy the volume data into native cloud block storage (SSD or magnetic tiers). The result will be a new independent VM that does not rely on any volumes presented from a VDP appliance.

Highlights

- Customers can easily migrate VMs and physical servers from on-prem to a cloud environment, or between cloud platforms.
- When using cloud as a DR environment, customers can decide at time of DR failover whether to run VMs from a VDP using instant-mount or copy the data to cloud native storage and run directly from that.

NFS datastore support with VMware (alternative to iSCSI)

Users of VDP can leverage NFS protocol, in addition to iSCSI as an alternative, when recovering VMs and applications in a VMware environment. VMs are captured over the network using VMware VADP and can now be mounted back to an ESX host using NFS protocol.

In addition, staging disks and recovered applications mounted into a VM (using a connector) can also be mounted to the ESX host over NFS and then presented as block devices (VMDK) to the VM. This applies to Windows and Linux and all supported applications, including SQL Server, Oracle, Linux-based databases captured with the CBT driver, and file systems.

Highlights

- More flexibility to capture and access data over NFS protocol.
- NFS can be easier to configure than block protocols in some environments.

NFS mount to Oracle RAC

Oracle ASM databases captured into a file system staging disk over NFS can now be mounted into a RAC environment. This allows the creation of virtual clones in a test/development environment with RAC, without having to restore the data back into an ASM database.

Highlights

- More flexibility to capture and access data over NFS protocol.
- Short RTO when accessing virtual clones (mounts) since data does not need to be restore from a file system image into an ASM format.

Clone SQL Server to another server

Allow user to recover SQL Server databases by copying the data to another server. The original database configuration is maintained. This is different from a mount: the data is copied to another storage rather than being presented from a VDP appliance. Full support from AGM.

Highlights

Recover SQL Server databases back to a point in time, copying data into production storage using original database configuration.

Enhanced Cyber-Resiliency leveraging IBM Cloud Object Storage (COS) Retention Capabilities

Users can designate backups as immutable by setting an option in a template policy. When this is set, no Actifio user can expire an image before its policy-driven expiration date, not even an administrator (this was available in v8.1).

Customers who use VDP with IBM Cloud Object Storage can now leverage its retention capabilities to add another layer of protection at the storage level in addition to the VDP level.

Highlights

Increase resiliency of data by protecting it from rogue users or malware/ransomware.

Enhanced call-home functionality

Appliance Call-Home can now leverage HTTPS protocol in addition to email.

Highlights

Simpler setup and enhanced security.

Managed Data License (MDL) calculation for VSAN

The calculation of Managed Data License has been enhanced to accurately reflect usage in a VMware VSAN environment.

Expanded support matrix

Added support for:

- Oracle 18
- Oracle and file system capture on Ubuntu systems. This does not include support for other applications using the change-block tracking driver.

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.

- o Support for databases and other generic applications on Linux using the change-block tracking driver.
- o Ability to export the content displayed in various grids (application list, host list, etc.) to CSV or PDF files
- o Streamlined display and management of application details & settings, including showing defaults and easily restoring defaults.
- o User can easily look up job failure errors in ActifioNOW knowledgebase, directly from System Monitor job details.
- o All table displays use a consistent grid component with standard, rich functionality.
- o 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.

VDP Features and Functions Not Supported in AGM 9.0

AGM 9.0 supports most of the features and functions available in the recent VDP releases. Features and functions not currently supported by AGM 9.0 can be performed at the VDP Desktop.

The following list summarizes the features and functions that are not part of AGM 9.0.

- **“Guardrails” to Provide Alerts and Warnings on Usage of System Resources:** Improved visibility into the impact that various configuration changes will have on a VDP appliance.
- **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.
- **Hyper-V Support:** Fully integrated support for managing, capturing, accessing, and restoring Hyper-V VMs.
- **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.

Limitations and Restrictions in AGM 9.0

Note: Features and functions not currently supported by AGM 9.0 are summarized in [VDP Features and Functions Not Supported in AGM 9.0](#).

- 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 upgrade process will appear to stop when running in Internet Explorer. The upgrade process continues to execute and will complete, however no status messages or updates will be displayed. [28140]
 - 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 does not immediately display when viewing in Internet Explorer. If you redirect the cursor to another area in the lower left-hand corner the version number will then appear. [30466]

Workaround: If you find that you are experiencing one or more of the issues outlined above, we recommend that you switch to a different browser such as Google Chrome or Mozilla Firefox to use the AGM UI.

- 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. [28419]

Workaround: Refresh the Active Image list and the appropriate operations will be shown.
- 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 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. [20533]
- After you add a VDP 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 VDP appliance on which they were created.[22747]

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**).
- The Applications window in the Applications 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 Application Manager from the VDP Desktop [24439, 24449, 24442, 24410].
- 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]

- 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]

- 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]
- Note the following object import considerations for organizations, users, and roles when you add a VDP appliance to AGM:
 - o 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 and will only be visible to the admin user on AGM. We recommend that you review all imported logical groups after importing and, if necessary, reassign them to the proper organizations. [22138]
 - o VDP appliance users who are 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]

Resolved Defects in AGM 9.0

The following list summarizes the resolved defects in AGM 9.0:

Resolved Defects

Issue	Fix	Tracking
Appliance version shows as "Not Available" after the appliance is added to AGM. This is because the system clocks for the appliance and AGM may not be in sync.	Issue should get resolved within thirty (30) minutes of adding the appliance, after which the appliance version should be available.	62012
If setting a SQL Instance to "Include System" while one or more system databases are ineligible, and those databases later become eligible, the SQL Instance inclusion rule may need to be reconfigured to get the system databases to be included. Databases are ineligible when they are individually managed, or included in a consistency group.		61878
Restricted shell vulnerability has been fixed; AGM no longer allows creation of user 'eng' or 'act' in order to protect those special accounts.		61807
For Oracle applications, the add and edit workflow pages show the following mapping options by default: Preferred Diskgroup Name and RAC Node list. These options are also available in the run workflow page when the selected source image is in ASM format.		61032, 36581
In certain situations, the Timeline Ramp View of an image was overlapping or truncating the actions drop-down menu, as a result of which the user could not select the desired mount, clone, restore, or any other action item.	Issue has been fixed and all menu items can be properly accessed.	60699
For SQL Instances, AGM shows correct data in the database inclusion rule for a disabled SLA.		60683
User may see an active image in the Active Image list but no associated image on the Timeline of the Application Manager's Access page.		60291
In certain situations, user may see an active image but no associated image on the timeline.		60259
AGM was not letting users rediscover the same VM after migration across vCenter.	The VM Onboarding Wizard introduced in AG 8.1.2 allows users to resync the details of a VM. In the Select Virtual Machines page of the wizard, a user can select "All VMs" filter. This will allow the user to rediscover the same VMs.	60155
The Job Details page in AGM System Monitor shows the Consistency Mode information. For example, Consistency Mode = "crash-consistent".		60145
Several enhancements have been made to the System Monitor jobs list view page. It has new filters "Application Type" and "Template" to filter jobs for better results. The Jobs list view has a new column "Application Type", which is hidden by default.		59969

Resolved Defects

Issue	Fix	Tracking
User was unable to create a user who had "-" in the email ID. Issue has been fixed and user with email ID abc-user@abc.com, for example, can be created.		59877
After successfully importing an appliance, AGM showed a blank screen.	AGM no longer shows a blank screen after an appliance import.	59749
Garbage collection progress can be monitored in the AGM UI.		59586
The Job Details page in AGM System Monitor has a new filter "Application Type". Users can refine the job list and view jobs for specific application types like Oracle, Exchange, or FileSystem.		59569
AGM user was unable to mount Exchange database to Exchange DAG server.	Mount and unmount of Exchange database to and from Exchange DAG server can be performed successfully.	59416
In AGM Domain Manager's LDAP Group Mapping page, the filter by option has been updated to "LDAP Group Name".		58988
The "Enable Sharing" option that was missing when "Join Appliance" was selected from Appliance Manager in the Appliance Settings page is now available.		58919
Volumes that are missing metadata (unique ID) are skipped from restore operations.		58813
AGM CLI command to create policyoption without specifying the required policy ID parameter threw a NullPointerException.	If a user tries to create a policyoption without specifying the policy ID, they will see the error message: Argument policyid required to create policyoption.	58811
Non-Admin user is no longer able to see the VMs that are managed by an Admin user.		58767
If the LDAP login was enabled, and the user tried to change the login credentials from the GUI, the following error/warning was shown: "LDAP group role mappings is enabled and therefore an individual user's role association cannot be updated manually".	AGM now allows users to update login credentials even when LDAP login is enabled.	58754
VMs that are ignored in one appliance are now discoverable in another appliance. Previously VMs ignored in one appliance were not displayed on other appliances as well.		58579
A cross-site scripting vulnerability detected in the Jobs view of AGM System Monitor has been fixed.		58322

Resolved Defects

Issue	Fix	Tracking
AGM web service 8.1.2 and later versions support only TLSv1.2 with following cipher suites: ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA		58280
AGM user without LiveClone manage rights was able to erroneously run a LiveClone backup.	User without LiveClone manage rights will no longer be able to perform a LiveClone backup. They will see the message: "User Does Not Have Sufficient Rights To Perform This Action".	58061
The Copy Data List page in AGM's Application Manager has a new column "Label" to show image labels.		58024
AGM logrotate now uses the correct configuration file with /etc/logrotate.conf file correctly pointing to /act/etc/logrotate.conf file. An issue of a missing softlink has been fixed.		57976
AGM logrotate compression has been updated to use bz2 compression.		57973
AGM logrotate configuration has been fixed to retain logs for 28 days instead of 4 days with log rotation frequency changed to daily rotation.		57970
AGM disables SELINUX during upgrade.		57964
Logical group with large number of applications was showing only eleven (11) applications.	Issue has been resolved and this restriction has been removed. All applications belonging a Logical group are now shown.	57706
AGM shows the system ID with label "SysID" along with the AGM version on left-hand service menu.		57603
New option "RAC Node List" has been added to support the backup of Oracle databases under NFS to mount as RAC.		57598
System State Recovery is not showing Storage Pool (Snapshot) option.	It now shows the Storage Pool option.	57529

Resolved Defects

Issue	Fix	Tracking
A performance issue has been addressed in Management Object Replication so that operations associated with SQL instances with a large number of members execute efficiently and do not cause long delays.		57518
Sensitive information contained in the catalogindexpassword policyoption created or updated from AGM were getting exposed as plain text content in the AGM database policyoption table. The same information was also getting exposed when using AGM CLI command udsinfo lspolicyoption.	Sensitive information in the catalogindexpassword policyoption are now encrypted, they are no longer exposed as plain text content.	57227
During Application consolidation, child applications and non-child applications with same names were getting consolidated.	An extra check for "parentid" has been introduced. As a result, during application consolidation: ***Child applications and non-child applications with same names no longer get consolidated; they show as different applications. ***Regular application and its shadow application created by DAR/Steamsnap are consolidated as one application. ***Child application and its shadow application created by DAR/Streamsnap are consolidated as one application. ***New VMs from multiple appliances will continue to be consolidated. New VMs from multiple appliances will continue to be consolidated.	57116
AGM System Monitor page has a new column, "TargetHost" that shows useful information about mount and about snapshot jobs of VMs. This information is useful in troubleshooting issues localized to a specific ESX host. The "TargetHost" column is not available in the default view. Users can enable the column for display.		57037
If a database that is part of SQL instance is individually protected, AGM now permits workflows for this database to be created and managed independently. Previously, users were forced to manage workflows at the level of the SQL Instance.		56714
Workflows configured for SQL databases or instances were not starting when user clicked on Submit on the Run Now page.	Workflows configured for SQL databases or instances now run correctly.	56650
When there is a communication failure between AGM and any appliance such that the array connectivity test cannot run, then the storage arrays show up as Red and there is an error message that explains why they are red.		56603

Resolved Defects

Issue	Fix	Tracking
Running AGM CLI commands mkldapserver, chldapserver and testldapserver exposed the lookup user's password in plain text in audit log. During an AppAware mount or when performing a preflight check, the password used for provisioning options was exposed in plain text in audit log.	Passwords are no longer exposed in the audit records.	56542
Issue with AGM showing a blank screen when user canceled a running job has been fixed.		56480
Documentation has been updated to note that there is no minimum size for external snapshot pool. Install sets up a 1 TB initial snapshot pool, but this is not the minimum limit.		56361
Due to a regression, AGM was not providing system recovery image details causing unmount operation to fail.	Issue has been fixed to send appropriate payload.	56337
Remote dedup mount failed when performing disaster recovery from AGM.	Issue has been fixed. Users can successfully perform remote dedup mount during disaster recovery from AGM.	56331
AGM inadvertently exposed the vCenter or ESX server login credentials in the AGM mom.log during Catalog file recovery or during host creation (both scenarios required user to test connectivity and validate user credentials). Exposure was limited to users with root account.	Enhancements have been made so that the login credentials are no longer exposed in AGM mom.log.	56282
If the target host for a file recovery from catalog is a VM, the File recovery option is disabled unless the existing connector at the target host supports recovery. This behavior applies to Windows hosts as well as Linux hosts.		56155
Added ability to delete hosts with very long names.		56090
A regression introduced by auditing improvements may have exposed the administrative credentials used to import an appliance to AGM.	Enhancements have been made to mask the login credentials in the audit records. You are advised to change the login credentials if login credentials were exposed.	56087
AGM user was not able to update password from within AGM. The old password persisted.	AGM users can update their own passwords.	56033
In the Application Manager page, the Application Name, Host Name and Friendly Path filters are collapsed by default.		55828

Resolved Defects

Issue	Fix	Tracking
For applications discovered on multiple appliances, user interface enhancements to show an ellipsis when appliance name or IP Address is long. Additional tool-tip to show the full name of the appliances and IP Address when user hovers the mouse over the name or IP Address.		55782
Application name was missing in the "Application Discovered on Multiple Appliances" pop-up.	Application name is now listed.	55781
Incorrect number of running jobs were displayed in the Job status pane of AGM Dashboard page. It was showing all running jobs instead of jobs started in the past day.	The Job status pane of AGM Dashboard page shows the correct number of running jobs (only those jobs that were started in the past day).	55622
In the Timeline view for backup images, the label showing the backup date to the left of the ramp did not match the backup date on the image.	Issue has been fixed. The backup date to the left of the ramp matches the backup date on the image.	55480
Under certain circumstances, depending on the LDAP server data model, calculating a LDAP user's group membership failed. This left the AGM user with no associated role and/or organization, as a result of which the user could not perform any operations.	Issue has been fixed.	55462
The option "Power on VM after mount" is now selected as the default option in the window when Mount as New Virtual Machine option is selected.		55419
In the Timeline view for backup images, the label showing the backup date to the left of the ramp did not match the backup date on the image.	Issue has been fixed. The backup date to the left of the ramp matches the backup date on the image.	55240
While importing OnVault images, AGM server timed out if the operation took more than five (5) minutes.	AGM server no longer times out when importing OnVault images.	55238
When configuring Workflows for an application running on a Windows server with Clustered and Standalone SQL Instances discovered in them, the correct mapping options (like Map to all ESXi Clusters, vRDM (default), and Mark Dependent) are now available.		54492
Added ability to add hosts by FQDN as an alternative to providing IP address, leveraging DNS for resolution.		54675
Users can access Access Manager page only if they have the correct permissions.		51747
When users without access to sensitive images create new workflow pages, they are no longer able to see sensitive images that they do not have access to.		48919

Resolved Defects

Issue	Fix	Tracking
Importing an OnVault image to a remote appliance from Application Manager was failing.	Issue has been fixed.	48003
During browser refresh, job filter selection for the past week/month was getting reset to the default filter of past day.	AGM retains the filter settings selected by the user after a browser refresh.	46375
In the previous fix of this defect, we fixed an issue where a failure was getting reported even when an SLA was successfully updated. Subsequently, a new issue was observed where AGM was displaying out of date content when even though the SLA update was successful. Additional fix for the new issue is available in this release.		45981
AGM is compressing log files in the bzip2 format.		44856
AGM error messages no longer reveal the PostgreSQL version.		44695
User was not able to monitor jobs (like Mount, create LiveClone etc.) running on remote images as they were not getting displayed in the System Monitor.	AGM displays jobs running on remote images as long as the application on which the original job ran or its host is in same organization as the user.	43562
When mounting an application aware Oracle database, the prep mount page now lists the application aware mount options that were previously missing.		41588
When modifying (viewing/removing) a consistency group containing a large number of applications (several hundred or more), there is no delay in the response time.		37649
During a mount operation, AGM did not prevent a user from selecting the Primary pool which could have resulted in unpredictable impact on the VDP appliance's operation.	When mounting captured data, the user can only select the performance pool by default.	37059
Clicking the "ASM Rebalance" option for unswitched Oracle ASM images shows an error message as there are no ASM devices to retrieve.		34724
Mounted StreamSnap® images application's Copy Data List table showed StreamSnap image as DAR in the "Image Details" view. However, the information was correctly displayed from the Copy Data Ramp view.	This cosmetic issue has been fixed.	34356
StreamSnap policy details are now correctly displayed in Manage SLA page.		33875
ESX Hosts are no longer getting listed as target hosts for failover, test failover, prep mount, clone jobs. It is also no longer listed as target host for mount and remount jobs where the appliance is not enabled allow mount to ESX host.		33714

Resolved Defects

Issue	Fix	Tracking
AGM System Monitor Job Type filter has three new options: ASM Switch and ASM Rebalance and ASM Rebalance Undo.		33680
The Ramp view showed the latest StreamSnap image in the correct location. However, the previous StreamSnap images were placed on the local SnapShot ramp location.	The issue has been fixed and the latest as well as the remote StreamSnap images are placed in the correct location.	33510
The Copy Data List view of the Access page of Application Manager shows "Image Type" column name instead of "Job Type". Users can filter on individual image types like Snapshot, OnVault and so on.		33027
The App ID column is available in the new application list grid. By default, it is hidden. For Applications that exist on multiple appliances have a "group" icon. Clicking on the icon shows a dialog listing the id for each of the applications.		31696
AGM System Monitor Job Type filter has a new option: Delete Test to delete test failed over images.		31088
An application that was remotely replicated from one appliance to another was being incorrectly displayed as 'Discovered on Multiple appliances'.	This issue has been fixed and the application is displayed only once on the appliance where it was originally discovered.	30761
The Application Discovered on Multiple Appliances popup dialog no longer have Appliance names overlapping with Host IP information.		30732
AGM user can now assign "ALL" organization category to either users or LDAP group mappings.		30395
AGM user could select and delete multiple Active Images.	The UI does not allow the user to perform any action after multiple Active Image selection. The user has to select an individual Active Image and choose to perform either Unmount or Unmount & Delete operations.	28642
When removing an appliance from AGM, a spinner indicates that the appliance is being removed. Upon successful removal, the following message is shown: "Removed appliance xxxxxxxx successfully."		27387

8 Known Issues

This section lists the known issues in the Actifio Global Manager (AGM) 9.0.7 release.

[Known Defects in AGM 9.0.7](#): on page 67

Known Defects in AGM 9.0.7:

The following list summarizes the known defects in AGM 9.0.7:

Known Defects

Issue	Workaround	Tracking
AGM		
An HTTP 404 error is shown when trying to reload the Appliance Configuration pages for an appliance running 9.0 SP1.	Workaround: Relaunch the Appliance Configuration pages from AGM or upgrade the appliance to a newer version.	72010
In the AGM Domain Manager, 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.	71868
VMware 6.7 Update 3 and higher cannot deploy Actifio OVA files due to VMware's choice to make implement a different hashing algorithm, and to block the previous one. Actifio OVA files can be converted using the VMware tool "ovftool" to change SHA1 to SHA256, and then may deploy the OVA file.	Issue will be addressed with an update to either VMware or Actifio in future releases.	71834
SQL Server Clone jobs initiated via AGM will not use NFS.	Run the clone operation from the command line on the appliance directly, or upgrade AGM to version 10c.	71568
Unable to add or edit appliances in the Edit Storage Array page.	Issue will be fixed in a future release.	70810
During an upgrade, the user may see the login to AGM message while the upgrade is still in progress.	Issue will be fixed in a future release.	68375

Known Defects

Issue	Workaround	Tracking
Removing the disk allocated for the reporting service will break AGM functionality.	Do not remove this disk. Contact Customer Success if you want to remove the reporting service.	66347
Saving a consistency group with 2,000 databases can take more than a few minutes.	Issue will be fixed in a future release.	63707
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 sometime (twenty minutes approximately), to let the upgrade process finish. Then login to the upgraded AGM.	62204
AGM Dashboard is not showing Managed Data information when the appliance filter is applied	Issue will be fixed in a future release.	61948
With certain paired appliances in sharing mode, there exists an edge case defect 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.	56637
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.	48690
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 any more. 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.	41869
VMware guest tools may not start after an AGM upgrade.	If you require VMware guest tools, contact your Actifio support representative.	37096

Known Defects

Issue	Workaround	Tracking
<p>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.</p> <p>Example error:</p> <ul style="list-style-type: none"> • Template: snaponly • Policy: snap • Field: iscontinuousincoming value: trueexisting value: null <p>Hot Fix 1099 addressed issues associated with policies with window duration longer than 23 hours and 50 minutes with a schedule type of daily.</p>	<p>To resolve this issue, you must remove the conflicting policies from AGM, apply HotFix 1199 to the Actifio appliance, and then re-import the Actifio 7.1.0 appliance to AGM.</p>	37042
<p>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.</p> <p>After waiting a few minutes, AGM will mark the Actifio appliance as Stale and the application list page performance will return to normal.</p> <hr/> <p>Note: <i>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.</i></p> <hr/> <p>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.</p>	<p>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.</p> <p>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.</p>	36821
<p>When multiple Organizations are selected in the AGM Domain Manager:</p> <ul style="list-style-type: none"> • 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. 	<p>Do not use the Edit option when multiple Organizations are selected.</p> <p>When you need to delete multiple Organizations, delete one Organization at a time.</p>	36444

Known Defects

Issue	Workaround	Tracking
<p>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.</p> <p>After both appliances are added, updated templates can be pushed to both appliances.</p> <p>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.</p>	Such errors are benign and can be ignored.	35483
<p>The ASM Switch radio button option can be displayed for images that are not eligible for ASM Switch.</p> <p>In AGM 8.0, when restoring some images from Actifio Sky 8.0.x appliances, the wrong backup image attribute is being checked and the ASM Switch option is shown for some images that are ineligible for that operation. This includes images captured to an ASM staging disk.</p> <p>In such cases, if you select the ASM Switch option, the AGM pre-flight test will run and then fail with an error. For example:</p> <p>ACTERR-010023 oracle user is not set, could be a older backup image.</p>	You should only perform ASM Switch on images that were captured after an Actifio appliance and connectors were upgraded to 8.0.	32971

Reporting

The application details section of the Snapshot Pool Consumption report does not include external snapshot pool data.	No known workaround.	62958
Changes made to saved options do not affect existing scheduled jobs.	Create a new schedule.	62791
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.	Known limitation.	53938
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.	No known workaround.	27933
Daily Protection Status report has some issues with horizontal scrolling in HTML view.	No known workaround.	27713

Known Defects

Issue	Workaround	Tracking
Actifio Report Manager does not work properly if your browser is configured with 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.	
<p>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]</p> <ul style="list-style-type: none"> 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

9 Security and Vulnerability Issues

This section lists security and vulnerability fixes for common names for vulnerabilities and exposures (CVEs) resolved as of this release. It includes the following topics:

- [Security Fixes in AGM 9.0.7](#) on page 73
- [CVEs Fixed in AGM 9.0.7](#) on page 75
- [Known Security, WhiteSource and CVE Issues in AGM 9.0.7](#) on page 84

Security Fixes in AGM 9.0.7

The following security issues were fixed in AGM 9.0.7

Security Fixes

Description	Fix	Fixed in	Tracking
The following high security vulnerabilities found during AGM upgrade have been resolved. <ul style="list-style-type: none">• CentOS Update for kernel CESA-2019:2863 centos6• CentOS Update for kernel CESA-2019:2736 centos6		AGM 9.0.5	77778
AGM audit data was leaking password in certain situations.	Issue has been resolved by sanitizing the password fields that were leaking.	AGM 9.0.5	77211
A serious vulnerability (CVE-2015-2080) in the Jetty Java Webserver used by AGM could allow an unauthenticated attacker to access a valid session token and potentially obtain unauthorized administrative access to AGM.	CVE-2015-2080 has been resolved. All AGM users are advised to upgrade as soon as possible.	AGM 9.0.5	76387
CentOS Update for java CESA-2019:3136 centos6		AGM 9.0.5	75607
The /tmp and /dumps folders are now installed with mount option protections "nosuid,nodev".		AGM 9.0.5	75058
CentOS 6 kernel has been updated in AGM to kernel packages announced via CESA-2019:2863 advisory.		AGM 9.0.5	72848

Security Fixes

Description	Fix	Fixed in	Tracking
Corrected high pam_faillock value.		AGM 9.0.5	72470
CentOS 6 kernel has been updated in AGM to kernel packages announced via CESA-2019:2736 advisory.		AGM 9.0.5	72328
The console.perms file has been removed from the security folder.		AGM 9.0.5	72249
SSH setting 'ClientAliveInterval' has been lowered.		AGM 9.0.5	72240
Unused HTTP options like DELETE, TRACK, TRACE have been removed.		AGM 9.0.5	72110
Postgres upgrade for the CVE-2019-10208 and CVE-2018-10915.		AGM 9.0.5	76726
Deprecated SSH MAC algorithm SHA1 has been replaced with SHA256.		AGM 9.0.5	72104
A potential SQL injection vulnerability in an API endpoint has been remediated.		AGM 9.0.4	71075
HTTP request redirections have been protected against forging attacks.		AGM 9.0.4	71057
Better security for sensitive information written to logs.		AGM 9.0.4	70175
Untrusted XML are now parsed without resolving external data.		AGM 9.0.4	71067
HTTP request redirections have been protected against forging attacks.		AGM 9.0.4	71057
CentOS Update for kernel CESA-2019:2473 centos6.		AGM 9.0.4	70924
CentOS Update for openssl CESA-2019:2471 centos6.		AGM 9.0.4	70663
AES encryption and decryption switched from AES/CBC/PKCS5Padding to AES/GCM/NoPadding due to security issues using Cipher Block Chaining (CBC) mode.	Encryption keys are now generated using AES with GCM mode instead of CBC and all the existing cipher text in upgrade scenarios is converted using AES with GCM mode.	AGM 9.0.4	68326
Error handling implementation in AGM was causing disclosure of sensitive information.	Issue has been fixed.	AGM 9.0.5	35932

CVEs Fixed in AGM 9.0.7

The following Common Vulnerabilities and Exposures (CVEs) were fixed in AGM 9.0.7:

Resolved CVEs

Description	CVE #
CiphertextHeader.java in Cryptacular 1.2.3, as used in Apereo CAS and other products, allows attackers to trigger excessive memory allocation during a decode operation, because the nonce array length associated with "new byte" may depend on untrusted input within the header of encoded data.	CVE-2020-7226
When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations. When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.	CVE-2020-1938

Resolved CVEs

Description	CVE #
In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.	CVE-2020-1935
When using FORM authentication with Apache Tomcat 9.0.0.M1 to 9.0.29, 8.5.0 to 8.5.49 and 7.0.0 to 7.0.98 there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability.	CVE-2019-17563
initDocumentParser in xml/XMLSchedulingDataProcessor.java in Terracotta Quartz Scheduler through 2.3.0 allows XXE attacks via a job description.	CVE-2019-13990
When Apache Tomcat 9.0.0.M1 to 9.0.28, 8.5.0 to 8.5.47, 7.0.0 and 7.0.97 is configured with the JMX Remote Lifecycle Listener, a local attacker without access to the Tomcat process or configuration files is able to manipulate the RMI registry to perform a man-in-the-middle attack to capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and gain complete control over the Tomcat instance.	CVE-2019-12418
A resource consumption vulnerability was discovered in apache-commons-compress in the way NioZipEncoding encodes filenames. Applications that use Compress to create archives, with one of the filenames within the archive being controlled by the user, may be vulnerable to this flaw. A remote attacker could exploit this flaw to cause an infinite loop during the archive creation, thus leading to a denial of service.	CVE-2019-12402
In version 2.0.3 Apache Santuario XML Security for Java, a caching mechanism was introduced to speed up creating new XML documents using a static pool of DocumentBuilders. However, if some untrusted code can register a malicious implementation with the thread context class loader first, then this implementation might be cached and re-used by Apache Santuario - XML Security for Java, leading to potential security flaws when validating signed documents, etc. The vulnerability affects Apache Santuario - XML Security for Java 2.0.x releases from 2.0.3 and all 2.1.x releases before 2.1.4.	CVE-2019-12400
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
Spring Security, versions 4.2.x up to 4.2.12, and older unsupported versions support plain text passwords using PlaintextPasswordEncoder. If an application using an affected version of Spring Security is leveraging PlaintextPasswordEncoder and a user has a null encoded password, a malicious user (or attacker) can authenticate using a password of "null".	CVE-2019-11272

Resolved CVEs

Description	CVE #
Some HTTP/2 implementations are vulnerable to a flood of empty frames, potentially leading to a denial of service. The attacker sends a stream of frames with an empty payload and without the end-of-stream flag. These frames can be DATA, HEADERS, CONTINUATION and/or PUSH_PROMISE. The peer spends time processing each frame disproportionate to attack bandwidth. This can consume excess CPU.	CVE-2019-9518
c3p0 version < 0.9.5.4 may be exploited by a billion laughs attack when loading XML configuration due to missing protections against recursive entity expansion when loading configuration.	CVE-2019-5427
Spring Security versions 4.2.x prior to 4.2.12, 5.0.x prior to 5.0.12, and 5.1.x prior to 5.1.5 contain an insecure randomness vulnerability when using SecureRandomFactoryBean#setSeed to configure a SecureRandom instance. In order to be impacted, an honest application must provide a seed and make the resulting random material available to an attacker for inspection.	CVE-2019-3795
When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disabled by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulfstange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).	CVE-2019-0232
Handling of the close_notify SSL/TLS message does not lead to a connection closure, leading the server to retain the socket opened and to have the client potentially receive clear text messages afterward. Mitigation: 2.0.20 users should migrate to 2.0.21, 2.1.0 users should migrate to 2.1.1. This issue affects: Apache MINA.	CVE-2019-0231
An issue is present in Apache ZooKeeper 1.0.0 to 3.4.13 and 3.5.0-alpha to 3.5.4-beta. ZooKeepers getACL() command doesn't check any permission when retrieves the ACLs of the requested node and returns all information contained in the ACL Id field as plaintext string. DigestAuthenticationProvider overloads the Id field with the hash value that is used for user authentication. As a consequence, if Digest Authentication is in use, the unsalted hash value will be disclosed by getACL() request for unauthenticated or unprivileged users.	CVE-2019-0201
The HTTP/2 implementation in Apache Tomcat 9.0.0.M1 to 9.0.14 and 8.5.0 to 8.5.37 accepted streams with excessive numbers of SETTINGS frames and also permitted clients to keep streams open without reading/writing request/response data. By keeping streams open for requests that utilised the Servlet API's blocking I/O, clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS.	CVE-2019-0199

Resolved CVEs

Description	CVE #
Square Retrofit version versions from (including) 2.0 and 2.5.0 (excluding) contains a Directory Traversal vulnerability in RequestBuilder class, method addPathParameter that can result in By manipulating the URL an attacker could add or delete resources otherwise unavailable to her.. This attack appear to be exploitable via An attacker should have access to an encoded path parameter on POST, PUT or DELETE request.. This vulnerability appears to have been fixed in 2.5.0 and later.	CVE-2018-1000850
Square Open Source Retrofit version Prior to commit 4a693c5aeeef2be6c7ecf80e7b5ec79f6ab59437 contains a XML External Entity (XXE) vulnerability in JAXB that can result in An attacker could use this to remotely read files from the file system or to perform SSRF. This vulnerability appears to have been fixed in After commit 4a693c5aeeef2be6c7ecf80e7b5ec79f6ab59437.	CVE-2018-1000844
dom4j version prior to version 2.1.1 contains a CWE-91: XML Injection vulnerability in Class: Element. Methods: addElement, addAttribute that can result in an attacker tampering with XML documents through XML injection. This attack appear to be exploitable via an attacker specifying attributes or elements in the XML document. This vulnerability appears to have been fixed in 2.1.1 or later.	CVE-2018-1000632
Legion of the Bouncy Castle Legion of the Bouncy Castle Java Cryptography APIs 1.58 up to but not including 1.60 contains a CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in XMSS/XMSS^MT private key deserialization that can result in Deserializing an XMSS/XMSS^MT private key can result in the execution of unexpected code. This attack appear to be exploitable via A handcrafted private key can include references to unexpected classes which will be picked up from the class path for the executing application. This vulnerability appears to have been fixed in 1.60 and later.	CVE-2018-1000613
A vulnerability was found in BouncyCastle. The number of iterations of the Miller-Rabin primality test was incorrectly calculated (according to FIPS 186-4 C.3). Under some circumstances, this could lead to the generation of weak RSA key pairs.	CVE-2018-1000180
Apache Thrift Java client library versions 0.5.0 through 0.11.0 can bypass SASL negotiation isComplete validation in the org.apache.thrift.transport.TSaslTransport class. An assert used to determine if the SASL handshake had successfully completed could be disabled in production settings making the validation incomplete.	CVE-2018-1320
A flaw was found in the way NSS responded to an SSLv2-compatible ClientHello with a ServerHello that had an all-zero random. A man-in-the-middle attacker could use this flaw in a passive replay attack.	CVE-2018-12384
The ntpq and ntpdc command-line utilities that are part of ntp package are vulnerable to stack-based buffer overflow via crafted hostname. Applications using these vulnerable utilities with an untrusted input may be potentially exploited, resulting in a crash or arbitrary code execution under privileges of that application.	CVE-2018-12327

Resolved CVEs

Description	CVE #
In Apache Batik 1.x before 1.10, when deserializing subclass of 'AbstractDocument', the class takes a string from the inputStream as the class name which then use it to call the no-arg constructor of the class. Fix was to check the class type before calling newInstance in deserialization.	CVE-2018-8013
A denial of service flaw was discovered in bind versions that include the "deny-answer-aliases" feature. This flaw may allow a remote attacker to trigger an INSIST assert in named leading to termination of the process and a denial of service condition.	CVE-2018-5740
A flaw named SegmentSmack was found in the way the Linux kernel handled specially crafted TCP packets. A remote attacker could use this flaw to trigger time and calculation expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() functions by sending specially modified packets within ongoing TCP sessions which could lead to a CPU saturation and hence a denial of service on the system. Maintaining the denial of service condition requires continuous two-way TCP sessions to a reachable open port, thus the attacks cannot be performed using spoofed IP addresses.	CVE-2018-5390
The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE-2016-4055.	CVE-2017-18214
In Apache Synapse, by default no authentication is required for Java Remote Method Invocation (RMI). So Apache Synapse 3.0.1 or all previous releases (3.0.0, 2.1.0, 2.0.0, 1.2, 1.1.2, 1.1.1) allows remote code execution attacks that can be performed by injecting specially crafted serialized objects. And the presence of Apache Commons Collections 3.2.1 (commons-collections-3.2.1.jar) or previous versions in Synapse distribution makes this exploitable. To mitigate the issue, we need to limit RMI access to trusted users only. Further upgrading to 3.0.1 version will eliminate the risk of having said Commons Collection version. In Synapse 3.0.1, Commons Collection has been updated to 3.2.2 version.	CVE-2017-15708
It was found that the Hotrod client in Infinispan would unsafely read deserialized data on information from the cache. An authenticated attacker could inject a malicious object into the data cache and attain deserialization on the client, and possibly conduct further attacks.	CVE-2017-15089
Apache POI in versions prior to release 3.17 are vulnerable to Denial of Service Attacks: 1) Infinite Loops while parsing crafted WMF, EMF, MSG and macros (POI bugs 61338 and 61294), and 2) Out of Memory Exceptions while parsing crafted DOC, PPT and XLS (POI bugs 52372 and 61295).	CVE-2017-12626
An issue was discovered in Pivotal Spring Web Flow through 2.4.5. Applications that do not change the value of the MvcViewFactoryCreator useSpringBinding property which is disabled by default (i.e., set to 'false') can be vulnerable to malicious EL expressions in view states that process form submissions but do not have a sub-element to declare explicit data binding property mappings. NOTE: this issue exists because of an incomplete fix for CVE-2017-4971.	CVE-2017-8039

Resolved CVEs

Description	CVE #
A vulnerability was found in spring-ldap that allows an attacker to authenticate with an arbitrary password. When spring-ldap connected to some LDAP servers, when no additional attributes are bound, when using LDAP BindAuthenticator with <code>org.springframework.ldap.core.support.DefaultTlsDirContextAuthenticationStrategy</code> as the authentication strategy, and when setting <code>userSearch</code> , authentication is allowed with an arbitrary password when the username is correct.	CVE-2017-8028
A flaw within the processing of ranged HTTP requests has been discovered in the range filter module of nginx. A remote attacker could possibly exploit this flaw to disclose parts of the cache file header, or, if used in combination with third party modules, disclose potentially sensitive memory by sending specially crafted HTTP requests.	CVE-2017-7529
A vulnerability was found in spring-ldap that allows an attacker to authenticate with an arbitrary password. When spring-ldap connected to some LDAP servers, when no additional attributes are bound, when using LDAP BindAuthenticator with <code>org.springframework.ldap.core.support.DefaultTlsDirContextAuthenticationStrategy</code> as the authentication strategy, and when setting <code>userSearch</code> , authentication is allowed with an arbitrary password when the username is correct.	CVE-2017-7525
In Apache FOP before 2.2, files lying on the filesystem of the server which uses FOP can be revealed to arbitrary users who send maliciously formed SVG files. The file types that can be shown depend on the user context in which the exploitable application is running. If the user is root a full compromise of the server - including confidential or sensitive files - would be possible. XXE can also be used to attack the availability of the server via denial of service as the references within a xml document can trivially trigger an amplification attack.	CVE-2017-5661
An issue was discovered in Pivotal SpringWeb Flow through 2.4.4. Applications that do not change the value of the <code>MvcViewFactoryCreator.useSpringBinding</code> property which is disabled by default (i.e., set to 'false') can be vulnerable to malicious EL expressions in view states that process form submissions but do not have a sub-element to declare explicit data binding property mappings.	CVE-2017-4971
In the Bouncy Castle JCE Provider version 1.55 and earlier the ECIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.	CVE-2016-1000352
In the Bouncy Castle JCE Provider version 1.55 and earlier the ECIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.	CVE-2016-1000346
In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES/ECIES CBC mode vulnerable to padding oracle attack. For BC 1.55 and older, in an environment where timings can be easily observed, it is possible with enough observations to identify when the decryption is failing due to padding.	CVE-2016-1000345
In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.	CVE-2016-1000344

Resolved CVEs

Description	CVE #
In the Bouncy Castle JCE Provider version 1.55 and earlier the DSA key pair generator generates a weak private key if used with default values. If the JCA key pair generator is not explicitly initialised with DSA parameters, 1.55 and earlier generates a private value assuming a 1024 bit key size. In earlier releases this can be dealt with by explicitly passing parameters to the key pair generator.	CVE-2016-1000343
In the Bouncy Castle JCE Provider version 1.55 and earlier ECDSA does not fully validate ASN.1 encoding of signature on verification. It is possible to inject extra elements in the sequence making up the signature and still have it validate, which in some cases may allow the introduction of 'invisible' data into a signed structure.	CVE-2016-1000342
In the Bouncy Castle JCE Provider version 1.55 and earlier DSA signature generation is vulnerable to timing attack. Where timings can be closely observed for the generation of signatures, the lack of blinding in 1.55, or earlier, may allow an attacker to gain information about the signature's k value and ultimately the private value as well.	CVE-2016-1000341
In the Bouncy Castle JCE Provider versions 1.51 to 1.55, a carry propagation bug was introduced in the implementation of squaring for several raw math classes have been fixed (org.bouncycastle.math.raw.Nat???). These classes are used by our custom elliptic curve implementations (org.bouncycastle.math.ec.custom.*), so there was the possibility of rare (in general usage) spurious calculations for elliptic curve scalar multiplications. Such errors would have been detected with high probability by the output validation for our scalar multipliers.	CVE-2016-1000340
In the Bouncy Castle JCE Provider version 1.55 and earlier the primary engine class used for AES was AESFastEngine. Due to the highly table driven approach used in the algorithm it turns out that if the data channel on the CPU can be monitored the lookup table accesses are sufficient to leak information on the AES key being used. There was also a leak in AESEngine although it was substantially less. AESEngine has been modified to remove any signs of leakage (testing carried out on Intel X86-64) and is now the primary AES class for the BC JCE provider from 1.56. Use of AESFastEngine is now only recommended where otherwise deemed appropriate.	CVE-2016-1000339
In Bouncy Castle JCE Provider version 1.55 and earlier the DSA does not fully validate ASN.1 encoding of signature on verification. It is possible to inject extra elements in the sequence making up the signature and still have it validate, which in some cases may allow the introduction of 'invisible' data into a signed structure.	CVE-2016-1000338
It was found that differences in the strictness of Spring Security, and Spring Framework request mapping could lead to resources not being secured. An attacker could use this flaw to bypass authentication.	CVE-2016-5007
A deserialization flaw allowing remote code execution was found in the BeanShell library. If BeanShell was on the classpath, it could permit code execution if another part of the application deserialized objects involving a specially constructed chain of classes. A remote attacker could use this flaw to execute arbitrary code with the permissions of the application using the BeanShell library.	CVE-2016-2510

Resolved CVEs

Description	CVE #
The duration function in the moment package before 2.11.2 for Node.js allows remote attackers to cause a denial of service (CPU consumption) via a long string, aka a "regular expression Denial of Service (ReDoS)."	CVE-2016-4055
The Realm implementations did not process the supplied password if the supplied user name did not exist. This made a timing attack possible to determine valid user names. Note that the default configuration includes the LockOutRealm which makes exploitation of this vulnerability harder.	CVE-2016-0762
The authenticated-encryption feature in the symmetric-encryption implementation in the OWASP Enterprise Security API (ESAPI) for Java 2.x before 2.1.0.1 does not properly resist tampering with serialized ciphertext, which makes it easier for remote attackers to bypass intended cryptographic protection mechanisms via an attack against the intended cipher mode in a non-default configuration, a different vulnerability than CVE-2013-5679.	CVE-2013-5960
It was found that the Apache commons-collections library permitted code execution when deserializing objects involving a specially constructed chain of classes. A remote attacker could use this flaw to execute arbitrary code with the permissions of the application using the commons-collections library.	CVE-2015-7501
Serialized-object interfaces in certain Cisco Collaboration and Social Media; Endpoint Clients and Client Software; Network Application, Service, and Acceleration; Network and Content Security Devices; Network Management and Provisioning; Routing and Switching - Enterprise and Service Provider; Unified Computing; Voice and Unified Communications Devices; Video, Streaming, TelePresence, and Transcoding Devices; Wireless; and Cisco Hosted Services products allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	CVE-2015-6420
The WLS Security component in Oracle WebLogic Server 10.3.6.0, 12.1.2.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to execute arbitrary commands via a crafted serialized Java object in T3 protocol traffic to TCP port 7001, related to oracle_common/modules/com.bea.core.apache.commons.collections.jar. NOTE: the scope of this CVE is limited to the WebLogic Server product.	CVE-2015-4852
It was found that the Java Standard Tag Library (JSTL) allowed the processing of untrusted XML documents to utilize external entity references, which could access resources on the host system and, potentially, allowing arbitrary code execution.	CVE-2015-0254,
The authenticated-encryption feature in the symmetric-encryption implementation in the OWASP Enterprise Security API (ESAPI) for Java 2.x before 2.1.0 does not properly resist tampering with serialized ciphertext, which makes it easier for remote attackers to bypass intended cryptographic protection mechanisms via an attack against authenticity in the default configuration, involving a null MAC and a zero MAC length.	CVE-2013-5679
A resource consumption issue was found in the way Xerces-J handled XML declarations. A remote attacker could use an XML document with a specially crafted declaration using a long pseudo-attribute name that, when parsed by an application using Xerces-J, would cause that application to use an excessive amount of CPU.	CVE-2013-4002

Resolved CVEs

Description	CVE #
Algorithmic complexity vulnerability in the sorting algorithms in bzip2 compressing stream (BZip2CompressorOutputStream) in Apache Commons Compress before 1.4.1 allows remote attackers to cause a denial of service (CPU consumption) via a file with many repeating inputs.	CVE-2012-2098
Apache Xerces2 Java Parser before 2.12.0 allows remote attackers to cause a denial of service (CPU consumption) via a crafted message to an XML service, which triggers hash table collisions.	CVE-2012-0881

Known Security, WhiteSource and CVE Issues in AGM 9.0.7

Security Issues

The following table lists the known security issues in AGM 9.0.7:

Known Security Issues

Description	Tracking
Self-signed certificates are not compatible with MacOS 10.15 Catalina. The issue will be fixed in an upcoming release.	77362
Some high security issues for Java, JavaScript, RPM libraries were detected. They will be fixed in an upcoming release.	77102
The value of the systemctl setting 'net.ipv4.conf.all.rp_filter' value remain the same.	72236

WhiteSource Issues

The following table lists the known WhiteSource issues in AGM 9.0.7:

Known WhiteSource Issues

Description	Tracking
XSS in data-target in bootstrap (3.3.7 and before)	WS-2018-0021
The class FileUploadBase in Apache Commons Fileupload before 1.4 has potential resource leak - InputStream not closed on exception.	WS-2014-0034
Apache commons-codec before version "commons-codec-1.13-RC1" is vulnerable to information disclosure due to Improper Input validation.	WS-2019-0379

CVE Issues

The following table lists the known CVE issues in AGM 9.0.7:

Known CVE Issues

Description	CVE #
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
Note: This vulnerability only applies to the optional catalog functionality of AGM.	

Known CVE Issues

Description	CVE #
<p>FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to <code>org.springframework.aop.config.MethodLocatingFactoryBean</code> (aka spring-aop).</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2020-11619
<p>A flaw was found in Netty in the way it handles the amount of data it compresses and decompresses. The Compression/Decompression codecs should enforce memory allocation size limits to avoid an Out of Memory Error (OOM) or exhaustion of the memory pool.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2020-11612
<p>FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to <code>org.apache.openjpa.ee.WASRegistryManagedRuntime</code> (aka openjpa).</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2020-11113
<p>FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to <code>org.apache.commons.proxy.provider.remoting.RmiProvider</code> (aka apache/commons-proxy).</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2020-11112
<p>FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to <code>org.apache.activemq.*</code> (aka activemq-jms, activemq-core, activemq-pool, and activemq-pool-jms).</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2020-11111
<p>In jQuery before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. <code>.html()</code>, <code>.append()</code>, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2020-11022

Known CVE Issues

Description	CVE #
<p>FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to javax.swing.JEditorPane.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p> <hr/>	CVE-2020-10969
<p>FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to javax.swing.JEditorPane.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p> <hr/>	CVE-2020-10968
<p>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.</p>	CVE-2020-10693
<p>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).</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p> <hr/>	CVE-2020-10673
<p>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).</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p> <hr/>	CVE-2020-10672
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p> <hr/>	CVE-2019-20445
<p>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."</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p> <hr/>	CVE-2019-20444

Known CVE Issues

Description	CVE #
<p>FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-20330
<p>Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-17571
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-17531
<p>A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLookup.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-17267
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-16943
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-16942

Known CVE Issues

Description	CVE #
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-16869
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-16335
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-14893
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-14892
<p>A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to com.zaxxer.hikari.HikariConfig.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-14540
<p>SubTypeValidator.java in FasterXML jackson-databind before 2.9.9.2 mishandles default typing when ehcache is used, leading to remote code execution.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-14379

Known CVE Issues

Description	CVE #
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-14439
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-12814
<p>In Apache POI up to 4.1.0, when using the tool XSSExportToXml to convert user-provided Microsoft Excel documents, a specially crafted document can allow an attacker to read files from the local filesystem or from internal network resources via XML External Entity (XXE) Processing.</p>	CVE-2019-12415
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-12384
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-12086
<p>A version of the Jackson JSON parser library is used that has a vulnerability that could allow maliciously crafted JSON to remotely execute. This vulnerability will be addressed in a following release.</p> <hr/> <p>Note: This vulnerability only applies to the optional catalog functionality of AGM.</p>	CVE-2019-10202

Known CVE Issues

Description	CVE #
A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-asl libraries but in different classes.	CVE-2019-10172
FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.AnterosDBCPCConfig (aka anteros-core).	CVE-2020-9548
Note: This vulnerability only applies to the optional catalog functionality of AGM.	
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
Note: This vulnerability only applies to the optional catalog functionality of AGM.	
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
Note: This vulnerability only applies to the optional catalog functionality of AGM.	
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
Note: This vulnerability only applies to the optional catalog functionality of AGM.	
In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.	CVE-2019-8331
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
Note: This vulnerability only applies to the optional Catalog functionality of AGM.	

Known CVE Issues

Description	CVE #
<p>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 <code>_aliases</code>, <code>_shrink</code>, or <code>_split</code> endpoints are used . If the <code>elasticsearch.yml</code> file has <code>xpack.security.dls_fls.enabled</code> set to <code>false</code>, 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.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2019-7611
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-1000873
In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.	CVE-2018-20677
In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.	CVE-2018-20676
<p>FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the <code>jboss-common-core</code> class from polymorphic deserialization.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-19362
<p>FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the <code>openjpa</code> class from polymorphic deserialization.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-19361
<p>FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the <code>axis2-transport-jms</code> class from polymorphic deserialization.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-19360

Known CVE Issues

Description	CVE #
<p>Lightbend Akka 2.5.x before 2.5.16 allows message disclosure and modification because of an RNG error. A random number generator is used in Akka Remoting for TLS (both classic and Artery Remoting). Akka allows configuration of custom random number generators. For historical reasons, Akka included the AES128CounterSecureRNG and AES256CounterSecureRNG random number generators. The implementations had a bug that caused the generated numbers to be repeated after only a few bytes. The custom RNG implementations were not configured by default but examples in the documentation showed (and therefore implicitly recommended) using the custom ones. This can be used by an attacker to compromise the communication if these random number generators are enabled in configuration. It would be possible to eavesdrop, replay, or modify the messages sent with Akka Remoting/Cluster.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-16115
<p>FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to conduct server-side request forgery (SSRF) attacks by leveraging failure to block the axis2-jaxws class from polymorphic deserialization.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-14721
<p>FasterXML jackson-databind 2.x before 2.9.7 might allow attackers to conduct external XML entity (XXE) attacks by leveraging failure to block unspecified JDK classes from polymorphic deserialization.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-14720
<p>FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the blaze-ds-opt and blaze-ds-core classes from polymorphic deserialization.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-14719
<p>FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the slf4j-ext class from polymorphic deserialization.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-14718
In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.	CVE-2018-14042
In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.	CVE-2018-14040

Known CVE Issues

Description	CVE #
<p>An issue was discovered in FasterXML jackson-databind prior to 2.7.9.4, 2.8.11.2, and 2.9.6. When Default Typing is enabled (either globally or for a specific property), the service has the Oracle JDBC jar in the classpath, and an attacker can provide an LDAP service to access, it is possible to make the service execute a malicious payload.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-12023
<p>A vulnerability was discovered in jackson-databind where it would permit deserialization of a malicious object using Jodd DB connection classes when using DefaultTyping. An attacker could use this flaw to achieve remote code execution under certain circumstances.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-12022
<p>When reading a specially crafted ZIP archive, the read method of Apache Commons Compress 1.7 to 1.17's ZipArchiveInputStream can fail to return the correct EOF indication after the end of the stream has been reached. When combined with a java.io.InputStreamReader this can lead to an infinite stream, which can be used to mount a denial of service attack against services that use Compress' zip package.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-11771
<p>An issue was discovered in FasterXML jackson-databind prior to 2.7.9.4, 2.8.11.2, and 2.9.6. When Default Typing is enabled (either globally or for a specific property), the service has the Jodd-db jar (for database access for the Jodd framework) in the classpath, and an attacker can provide an LDAP service to access, it is possible to make the service execute a malicious payload.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-11307
<p>Unbounded memory allocation in Google Guava 11.0 through 24.x before 24.1.1 allows remote attackers to conduct denial of service attacks against servers that depend on this library and deserialize attacker-provided data, because the AtomicDoubleArray class (when serialized with Java serialization) and the CompoundOrdering class (when serialized with GWT serialization) perform eager allocation without appropriate checks on what a client has sent and whether the data size is reasonable.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-10237

Known CVE Issues

Description	CVE #
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-7489
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-5968
<p>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.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-3831
<p>A specially crafted ZIP archive can be used to cause an infinite loop inside of Apache Commons Compress' extra field parser used by the ZipFile and ZipArchiveInputStream classes in versions 1.11 to 1.15. This can be used to mount a denial of service attack against services that use Compress' zip package.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-1324
<p>Spring Framework, versions 5.0 prior to 5.0.5 and versions 4.3 prior to 4.3.15 and older unsupported versions, provide client-side support for multipart requests. When Spring MVC or Spring WebFlux server application (server A) receives input from a remote client, and then uses that input to make a multipart request to another server (server B), it can be exposed to an attack, where an extra multipart is inserted in the content of the request from server A, causing server B to use the wrong value for a part it expects. This could lead to privilege escalation, for example, if the part content represents a username or user roles.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2018-1272

Known CVE Issues

Description	CVE #
<p>The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2017-18640
<p>A deserialization flaw was discovered in the jackson-databind which could allow an unauthenticated user to perform code execution by sending maliciously crafted input to the readValue method of ObjectMapper. This issue extends upon the previous flaws CVE-2017-7525 and CVE-2017-15095 by blacklisting more classes that could be used maliciously.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2017-17485
<p>A deserialization flaw was discovered in the jackson-databind 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.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2017-15095
<p>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=xmllparser 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.</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2017-12629
<p>In Hibernate Validator 5.2.x before 5.2.5 final, 5.3.x, and 5.4.x, it was found that when the security manager's reflective permissions, which allows it to access the private members of the class, are granted to Hibernate Validator, a potential privilege escalation can occur. By allowing the calling code to access those private members without the permission an attacker may be able to validate an invalid instance and access the private member value via ConstraintViolation#getInvalidValue().</p> <hr/> <p>Note: This vulnerability only applies to the optional Catalog functionality of AGM.</p>	CVE-2017-7536

Known CVE Issues

Description	CVE #
Pivotal Spring Framework 4.1.4 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required.	CVE-2016-100027
In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	CVE-2016-10735
Apache Struts 2.0.0 through 2.3.24.1 does not properly cache method references when used with OGNL before 3.0.12, which allows remote attackers to cause a denial of service (block access to a web site) via unspecified vectors.	CVE-2016-3093
mustache package before 2.2.1 for Node.js allows remote attackers to conduct cross-site scripting (XSS) attacks by leveraging a template with an attribute that is not quoted.	CVE-2015-8862
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
Note: This vulnerability only applies to the optional Catalog functionality of AGM.	
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
Note: This vulnerability only applies to the optional Catalog functionality of AGM.	