Avecto

Enterprise Reporting Release Notes

Software Version: 4.5.13.0 GA

Document Version: 1.0

Document Date: 30 May 2017

Ave1cto

Avecto

Table of Contents

Avecto

Chapter 1 - Release Notes

- **New Features** detailed below
- **Enhancements** detailed below
- **Bugs Fixed** detailed below

1.1 - New Features

50740 - Added database views for exporting Avecto Event data into SIEM products such as Splunk. Please see the Exported Views appendix in the Enterprise Reporting Dashboard Guide for more information.

1.2 - Enhancements

- **Database** detailed below
- **SSRS** detailed below

1.2.1 - Database

The performance of many reports in the suite has been improved.

48440 - The Enterprise Reporting database now has a version table called DatabaseVersion.

1.2.2 - SSRS

53265 - Enterprise Reporting has been tested with SQL 2016 and is compatible.

1.3 - Bugs Fixed

- **Database** detailed below
- **SSRS** detailed on the next page

1.3.1 - Database

52790 - The performance of the ApplicationReport and ApplicationsTable reports has been improved.

56820 - The ErpEventsAdmin report now loads when a limited permission user account is used.

58270 - The performance of the GetApplications procedure has been improved.

58560 - Updated the permissions so they are valid after upgrading from a 4.1 database to 4.3.

59152 - Fixed an issue that caused the Event Parser to crash while processing Logon events with future dates.

59406 - The performance of the GetMostRecentEventsFromHosts procedure has been improved.

60022 - The performance of the Summary dashboard has been improved.

61483 - Parameters that were missing from the permalink in the ItemList report have been added so the Policy ID is now in the URL.

63301, **51477** - The RemoveDuplicateHosts procedure has been removed. Hosts are now differentiated using their HostName so there are no duplicates.

1.3.2 - SSRS

Multiple fixes for drilldown inconsistencies.

53050 - Fixed an error that occurred when you drilled down from the By Operating System Type pie chart on the Deployments dashboard.

58637- Added COM Class to the advanced filter of the Discovery dashboard.

50872 - Drilling down from any Discovery table now shows the correct number of events as it now matches against the Distinct Application ID. The Distinct Application ID is also in the advanced filters and in the URL when a permalink is selected.

60779 - In the ERP Summary report, users who are both an admin user and a power user are now displayed after drilling down.

1.4 - Supported Operating Systems

- **Event Collector OS** detailed below
- **Database** detailed below
- **SQL Reporting Services (SSRS)** detailed below

1.4.1 - Event Collector OS

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

1.4.2 - Database

- SQL 2008 R2 Express
- SQL 2008 R2 Standard or Enterprise
- SQL 2012 Standard or Enterprise
- SQL 2014 Standard or Enterprise
- SQL 2016 Standard or Enterprise
- Azure SQL Server

1.4.3 - SQL Reporting Services (SSRS)

- SSRS 2008 R2 Express
- SSRS 2008 R2 Standard or Enterprise
- SSRS 2012 Standard or Enterprise
- SSRS 2014 Standard or Enterprise
- SSRS 2016 Standard or Enterprise

The SSRS version must match the SQL Server version.

Chapter 2 - Version History

2.1 - 4.3.144.0 SR1

2.1.1 - New Features

61532 – Added support for sudo events with a new Application type to allow import of sudo events into a Defendpoint policy.

61813 - SSRS Reports have been updated to display sudo control events using a new Application type.

2.1.2 - Bugs Fixed

61970 - Fixed a performance issue with database queries `GetApplicationChildren` and `GetApplicationParents`.

61740 - Fixed a performance issue that occurred when attempting to load a filter when using a larger database.

2.2 - 4.3.116.0 GA

2.2.1 - New Features

- Reporting for Mac OS X end-points added
- Reporting Performance improvements
- Removed help guide from within product as first step to online documentation that can be updated between releases. The latest guide is available in the Avecto Connect portal
- Azure SQL Server is now supported for use with iC3

2.2.2 - Bug Fixes

- Multiple fixes for chart and table drill down errors and inconsistencies
- Certain types of Privileged Accounts Protections events are now handled properly, which were the cause bad staging batches
- Added missing labels to Privileged Account Modifications report
- Fixed displaying of events on leap days
- Fixed purging of data older than 12 months
- Event parser installation now permits you to continue even if the account validation fails
- Fixed missing details in the Message distribution chart on the User Experience report for the 30-day range
- Fixed disappearance of other publishers on Discovery > Publisher when one was expanded

2.3 - 4.1.160

2.3.1 - Features

- Summary Dashboard - The Summary dashboard highlights the most important activity that occurred in the prior day, week or month. At a glance, the administrators are led to the policy adjustments and anomalies that require attention.

- Application Discovery Dashboards - The Discovery dashboards provide direct, summarized access to the applications that are newly observed in the preceding time period. The reports filter and group applications by common criteria such as requiring elevation, run from an external sources and the filesystem locations they ran from. These highly tailored views inform policy modification such as elevation rules or application whitelist additions.
- Streamlined Installation - The Event Management installer has been split into an Event Parser installer and a Database installer to simplify account permissions required for installation and to ease the process of setting up multiple event collectors

2.3.2 - Bugs

- Update stored procedures to handle Windows 10 version
- "Sandbox" filter parameter support for "Not set" option added UserSessions table LogonTime entries data value issue corrected
- Privileged Logons reports response time improved
- DistinctApplications.Description column is not wide enough for some URLs
- Multiple value filtering extended to all text parameters
- Charts displaying in UTC instead of local time

2.4 - 4.0.370 (SR2)

2.4.1 - Bug Fixes

- An exception in the HandleStagingError procedure can prevent CopyFromStaging processing any more rows. This occurred when the account running CopyFromStaging did not have permission to write to the SQL Server error log.
- Summary by process Activity (Top10)' bar chart on Workstyle dashboard does not count the workstyles if they have the same name.

2.5 - Known Issues

- When upgrading from 4.0 to 4.0SR2 the 4.0 reports in the existing folder in SSRS should be removed (deleted) prior to installing 4.0 SR2. This is due to a SSRS bug where reports are not always overwritten cleanly.

2.6 - 4.0.312 (SR1)

2.6.1 - Headline Changes

- Better error handling has been added to the "CopyFromStaging" process. In the event of an error the error is logged and the batch is stored for later review. See details below.
- Performance improvements to the "CopyFromStaging" process. The batch to be processed is now copied only once rather than three times. 10,000 rows are processed at a time rather than 1,000. Other optimisations have also been applied.
- Allow "CopyFromStaging" to be kept running for arbitrary amounts of time. This is to avoid having to call it every 10 seconds. See details below.
- Bug fix in the "CopyFromStaging" process where a call to the "RemoveDuplicateHosts" database sanitisation procedure was taking a long time to complete and the procedure was not achieving anything.
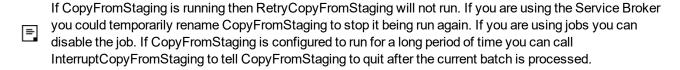
2.6.2 - Error Handling in Enterprise Reporting 4.0 SR1

- The event collector(s) insert event data into the Staging table. The stored procedure CopyFromStaging copies 10000 events from Staging into StagingTemp, then processes them and then deletes them.

- By default the Service Broker is set up to call CopyFromStaging every 10 seconds to process the data in the Staging table.
  - However some customers prefer to use the SQL Server Agent to run a job regularly.

- There is a script "Create_ERP_Database_Agent.sql" which removes the ServiceBroker objects and sets up a job to be run every 10 seconds. If the customer prefers to schedule the job less frequently then CopyFromStaging can be supplied with a parameter which is the minimum time in minutes for the procedure to run for. In this scenario the procedure will continue processing batches in a loop. After each batch it will check if it has exceeded the run time and quit if necessary. If the staging tables are empty it will sleep for 10 seconds before trying to process another batch.

- The script "Create_ERP_Database_Agent.sql" has two commented out lines which support the parameter for CopyFromStaging. They should be uncommented and the line above them commented out. By default the run duration is 10 minutes and the job is run every 12 minutes.

- The time between running the job should be longer then the CopyFromStaging run time as CopyFromStaging could run for longer than the given time. The SQL Server Agent will not try to start a job if it is already running.

- If an error occurs inside CopyFromStaging the batch in StagingTemp is copied to StagingTempBadBatches and the error message is stored in StagingErrors. Processing of new events will then continue as normal.

- If a batch has an error then the whole batch is copied into StagingTempBadBatches, not only the bad rows. In order to process the data in StagingTempBadBatches and leave only the bad rows you can call RetryCopyFromStaging. This will process the rows one at a time and leave only the offending ones.

If CopyFromStaging is running then RetryCopyFromStaging will not run. If you are using the Service Broker you could temporarily rename CopyFromStaging to stop it being run again. If you are using jobs you can disable the job. If CopyFromStaging is configured to run for a long period of time you can call InterruptCopyFromStaging to tell CopyFromStaging to quit after the current batch is processed.

2.7 - Bug Fixes

- The description is wrong for Content Events in the Events -> All report.
- Event Management Installation fails on Windows Server 2008.
- No event description for "199" events.
- Events > All report: No description for application launched using shell with authentication.
- Wrong process counts in top level dashboards when the same application has event s with the same event number but different token types.
- When upgrading the database from 3.8 to 4.0, some event types are not added to the summary tables.
- Requests Dashboard -Services missing in bar chart
- Workstyles Dashboard- When the "Summary by Process Activity (top 10)" shows the top 10 workstyles and a further workstyle (not in top 10) has more activity, the graph does not update.
- Events > All report: Logon events are also displayed along with application events
- CopyFromStaging can fail when there are duplicate StagingEntryGUIDs in Staging.
- CopyFromStaging_TokenAssignments fails when an event has a NULL TokenGUID.
- Defendpoint Service started events are not inserted into the database unless the domain is already in the Domains table.

- Add some form of locking to CopyFromStaging so that it cannot be run concurrently.
- After a CopyFromStaging error, MSFT SQL server error logs should be populated with a specific, useful error message.
- Enterprise Reporting rejects Authorization Challenge codes that are more than 8 digits long.
- Enterprise Reporting– Workstyles dashboard -Process coverage by Group Policy Object –the legend is overlaying the chart.
- Applications Dashboard can show wrong process counts in "top 10 application activities" chart.
- Filter Panel- User Name search filter doesn't work for TargetType > All.
- Reporting help file needs updating to Defendpoint 4.0

2.8 - 4.0.148

2.8.1 - New Features

- New Actions and Target Types dashboards to allow more detailed and more convenient investigations into application activity
- New EventsAdmin dashboard for data purging
- Support for new Sandbox and Content events
- New filter pane to allow one click filtering
- New User Experience dashboard
- New Requests dashboard and table
- New Events dashboard and table
- Improved flow around the reports –many cells in the Events > All table and the Event Report can be clicked to view the entity report.
- Ability to search using wildcards

2.8.2 - Enhancement

- Column sorting added to all tables
- Improved Policies charts
- Enhanced drilldowns

2.8.3 - Bug Fix

- Permalink issues fixed

2.9 - 3.8.285.0

2.9.1 - Bug Fix

- Fixed issue when importing pre 3.0 events into the database.

2.9.2 - Enhancement

- Performance improvements to report generation.

2.10 - 3.8.141.0

2.10.1 - Enhancement

- Improved Event Collection, Database and Reporting Pack installation process.

2.11 - 3.8.115.0

2.11.1 - New Features

- Added new dashboard for Privileged Account Protection
- Added Database purging utility to allow manual or scheduled purging of old event data.

2.11.2 - Enhancements

- Added support for Windows Store Applications.
- Added support for new Privilege Guard 3.8 features.
- Extended drilldown support to Privileged Logons, Deployments and Policies dashboards.
- Added data for non-default Access tokens to Policies dashboard.
- Added ability to filter on the 'Reason' event property.

2.11.3 - Bug Fixes

- Improved database upgrade scripts with better management of null fields.
- Numerous cosmetic improvements to dashboards and reports.

2.12 - 3.6.235.0

- No longer overwrite the domain name with "NT AUTHORITY" during data import
- Added functionality required for support of the Avecto Data Analyzer
- Fixed a problem with upgrades from earlier 3.6 releases

2.13 - Version 3.6.221.0

- Fixed an issue which can occur when upgrading from a version of Enterprise Reporting prior to version 3.6.

2.14 - 3.6.201.0

2.14.1 - New Features

- Updated look & feel, with improved drilldown support and report filtering.
- Updated Applications dashboard with logical grouping reports.
- New Discovery dashboard.
- New Privileged Logons dashboard.
- New Deployments dashboard.
- New Policies dashboard.
- New item summary reports for applications, processes, users, hosts and policies.
- New Processes dashboard with granular events table.
- Added permalinks to each dashboard and report, allowing direct access to custom filtered views.

- Added parent and child relationship reports to application and process summary reports.
- Optimized report generation performance.
- Added error event logging in the Event Parser service.
- Added support for comma separated filtering in User Name, Host Name, Policy and
- Application Description filters.

2.15 - 3.5.181.0

2.15.1 - Bug Fixes

- Added performance improvements to the database and SSRS reports.
- Fixed an installer bug that caused an upgrade failure if database was not named 'AvectoPrivilegeGuard'.

2.16 - 3.5.163.0

2.16.1 - Bug Fixes

- Added extra resilience to the database connection management in the Event Parser service to better handle network and server outages.

2.17 - 3.5.15.0

2.17.1 - New Features

- New Health Dashboard, which reports privileged user logons and Privilege Guard client installations.

2.17.2 - Bug Fixes

- Fixed the report footers so the date and time is displayed using the correct regional format.
- Report table sorting is now applied to all pages.
- Authorizing User information is now displayed and formatted correctly.
- Long Custom Token descriptions are now displayed correctly in the reports.
- Long product descriptions no longer cause malformation of the 'Top 10' charts.
- Fixed formatting of the Discovered Applications chart when a large number of discovered applications are displayed.
- Removed hyperlink formatting from reports exported to PDF.
- Added support for substring matching in the report filters (where relevant).

2.18 - 3.0.310.0

- Fixed an issue in the event parser where a small number of events may not be added to the database.

2.19 - 3.0.291.0

2.19.1 - New Features

- Privilege Guard Event Collector aggregates and uploads events to the database Trend analysis reports:
  - Applications which require elevated privileges
  - Applications executed, and applications blocked

- Applications by user, by type, by time period
- Policy elevated vs On Demand elevated
- Identification of unique applications

- Rich interactive dashboard reports:
    - Top 10 applications executed, elevated, blocked
    - Top 10 Users, Vendors,
    - Elevation by type
    - Events by ID