Guardium Big Data Intelligence Version 4.1 - Release Notes

SonarFinder and SonarDispatcher

- Fix "unable to save" issue when URL field is empty and WSURL is empty
- Allow storing SMTP credentials with empty Username and/or Password
- Fix issue where only first of scheduled multi-jobs was respecting $$LAST_DID
- Make Group-Members a view by default to allow local group editing
- Fix overflow of large string with $out to CSV
- Support getting credentials via sonarconnection endpoints in SonarDispatcher
- support SSL option for Oracle connections in SonarDispatcher
- Change SonarDispatcher sleep time in each cycle from 30 seconds to 10 seconds
- Write target emails from emailToField in SonarDispatcher job documents
- Always use dynamic row height in pdf conversion
- SonarDispatcher support for RDBMS pull from Sybase
- SonarDispatcher Support for RDBMS pull from Teradata
- Add the ability to run customer python scripts from SonarDispatcher
- Add new set of ""sample"" files for dispatcher conf (instead of putting all samples inside the dispatcher.conf)
- SonarDispatcher support for email templates
- SonarDispatcher support for job chaining (dependencies)
- SonarDispatcher new canceled status for Jobs
- SonarDispatcher can now send data retrieved using RDBMS pulls to SonarGateway for enrichment and transformations
- If the recipient list is the same for all the lines in a SonarDispatcher job, generate only 1 csv/pdf
- Enable cleanup of r SonarDispatcher saved report files based on filter even for non-workflow jobs
- SonarDispatcher support for multiple database targets in RDBMS pulls/connections
- SonarDispatcher support for sending emails using non-English characters
- Move SonarDispatcher rsyslog config to a separate file
- Handle timestamp type with timezone offset from different RDBMS in SonarDispatcher
- SonarDispatcher handling of "/" in job names
- New SonarDispatcher control screens and add ability to "cancel" pending SonarDisptcher jobs
- Add the ability to define "email template" and save "formats" to be used by the SonarDispatcher emails
- Add services types drop down list to Cloud Sources screen

UEBA

IMPORTANT

Out-of-the box UEBA features may be overwritten during upgrade. If you need to preserve changes and configurations you've made to your existing installation, contact jSonar support.

- Improved performance of new entity flagging for conditional and peer models

- Alert only once for the same UEBA case
- Manage minimum sample size in UEBA models
- Create outlier alerts if the same behavior was previously a new entity
- Smart exclusion lists for UEBA and other applications
- Snooze alerts in EUBA allows configuring how quickly to resend alerts about same entities in UEBA
- Add additional feature details to UEBA discrete models
- Add lock user playbook info to default UEBA models
- Add min/max_outlier_value to default UEBA numeric models
- Add minimum behavior delta configuration to numeric UEBA models
- Add server type to details for all default UEBA models
- Remove outlier_score field from UEBA suspicious accounts creation model
- Remove score multipliers from UEBA models
- Separate the new entity alerts and outlier alerts
- Add lock user playbook info to default models
- Enhance details on UEBA Machine Takeover models
- Score normalization for UEBA suspicious grants and suspicious account creation
- UEBA SQL injection model
- Add drill down URLs in UEBA results
- Define z score when standard deviation is 0 in UEBA models
- UEBA Historical Numeric models' "score" should be 0 in case of entity is not outlier
- Score normalization for UEBA models
- Sort and limit are not applied to email alerts for outliers, but are applied to tickets and syslog alerts

Justify

- 'POST' option on Justify workflow trigger webservice
- Fix Workflow display of sub docs values
- Default table board for outlier incidents workflow in Justify
- Add new option in the Justify Trigger transition option, matched tickets only or custom match condition
- Allow workflow tickets in Justify to do transition from 'Any status'
- Change the default workflow configuration for all default UEBA models
- Drill downs in Outlier Incidents workflow in Justify to allow similar actions as in Threat Dashboard
- Add label option to transition info and event info in Justify
- Justify Trigger to update ueba_results with decisions from workflow

Sonargd

- Allow specifying separator and header separator in sonargd basic plugin
- Sonarg-setup-log is collected in collect-info
- Allow misc files with no extension
- Added copy plugin to sonargd
- Sonarremote PUSH option
- Add common fields and skip lines to sonargd basic csv plugin
- Ingest files are processed using multiple threads
- Add file name is included in sonargd ingest errors
- Sonargd ingest file failures move file to audit
- Sonargd ingest failures (after extraction) move the whole directory to audit
- Sonargd ingest plugin specifies the db in the command
- Sonargd skips non-extractable files (e.g. metadata snappy file)

HADR

- 3-node HADR configuration
- Fix HADR replication for databases with thousands of collections

System

- Reduced dependencies by static compilation
- Upgrade to Python 3.6
- Deprecate RHEL6 support

Cloud Support

- Support for AWS RDS Microsoft SQL Server
- Improve support for Snowflake – better handling of pagination and timing of pulls

SonarK

- Reactive Search in SonarK Discover allows the user to see incremental/partial results while they are still being built.
- SonarK lists on dashboards allow viewing distinct values
- SonarK support for custom names for indexes (instead of database-collection)
- SonarK upgrade underlying Kibana from v6.2.2 to v7.0.0.
- SonarK kills the existing query when changing the query in Discover or Dashboard.
- SonarK hides typed fields (ends with *_lmrm*) in Discover.
- SonarK replaces Sonar Aliases when selecting a new one in Discover/Dashboard.
- SonarK Index Management table is now listed in a paginated table with a search bar, as opposed to blindly listing them in the page.
- SonarK searching for visualization and dashboard is now faster and uses partial matching.
- SonarK adds performance warning when exporting PDF and doc count exceed 10000.
- SonarK fix for searching using Arabic characters

Pen-test fixes

- pen-test: (ase id: 459956) URLS may contain sensitive information
- pen-test: GBDI-126 Missing Cookie Secure Attribute
- pen-test: GBDI-129 Use of Hard-coded Credentials
- pen-test: GBDI-143 Using Components with Known Vulnerabilities
- pen-test: GBDI-144 Information Exposure

SonarW

- New $toObjectsAndVerbs operator in SonarGateway
- New Input sources in SonarGateway: * Splunk * MongoDB Atlas * Teradata * BigQuery * Marklogic * AWS S3 * Snowflake * AWS Kinesis * AWS MSSQL
- SonarGateway statistics for dashboard
- SonarGateway mapping updates for dynamodb, cloudera, oracle, kafka_consumer
- SonarGateway support for redaction of subdocuments
- Improved SonarGateway LEEF parsing
- SonarW $lmrm__metadata aggregation stage
- SonarW $top accumulator added to $group stage
- Various improvements for handling low and out of disk space in SonarW

- Graceful handling of MMAP errors in SonarW
- Added $flattenToSet operator in $group stage
- $tsearch with array in SonarW
- SonarW join on disk for supporting very large joins
- Added format option to $dateFromString in SonarW
- Prevent insertion to a column named "." in SonarW
- Improve DR connectivity email issue in SonarW
- Additional collstats in SonarW
- SonarW speedup for multicolumn selection with deleted docs
- Improve $unwind memory usage in SonarW
- SonarW allows producing oversized arrays that will not fit in bson by $facet followed by $unwind
- SonarW $in dies more quickly when killed
- SonarW $contains no longer generates error logs when invalid delimiter lengths are given
- SonarW save group documents on disk for very large groups
- SonarW continues query when bson is too large in addToSet, addToSetWithCount, flattenToSet.
- SonarW AES encrypt and decrypt: add salt as an optional 3rd parameter
- Support $out to syslog in pretty format in SonarW
- Fix overly aggressive cloud upload in SonarW

Guardium-Specific

- [jproxy] Adjust tar directory structure
- [jproxy] Readjust tar directory structure
- Pipelines and alerts for predicting when Guardium collectors will run out of disk space

SaaS-Specific

- Add extra endpoints to ngnix config when doing saas setup
- Administrator user has access to pages that shouldn't be user reachable
- Clean up snapshots
- Disable yum caching
- Generate appliance ID
- Generate random administrator password
- Lifecyle policy re-name
- Lifecyle policy includes more collections