Release Notes

==========

Product:	IBM Security Guardium Insights
Release version:	Guardium Insights 3.2.0
Completion date:	September 2022

IBM Security Guardium Insights is a hybrid cloud data security hub that helps you improve visibility into user data activity and risk. Guardium Insights helps you protect data more efficiently, enhance information technology flexibility, and reduce operational costs as you embrace new business paradigms (such as moving data to the cloud). Guardium Insights helps reduce the cost and complexity related to collecting, managing, and retaining data security and compliance data. It provides new analytics to enhance threat investigations - and it provides quick reporting functionality (including pre-built reports). Risk scoring and alerting in Guardium Insights help you prioritize your activities.

IBM Security Guardium Insights is a powerful tool that can help you secure your data. Simple to use, Guardium Insights allows you to set up connections to your data sources.

Guardium Insights provides tools to help you analyze data:

- Outlier mining: Detect anomalies in activities and exceptions.
- Risk events: Identify assets at risk using broad data points.
- Reports: Dive into the raw data for deep investigation.

Table of Contents

Download Guardium Insights v3.2.0

Guardium Insights V3.2.0 can be downloaded as an archive file (`2.2.0.tar.gz`) from:
https://github.com/IBM/cloud-pak/tree/master/repo/case/ibm-guardium-insights
You can install only the products for which your site is entitled.

For further instructions, read the README.md file located after unzipping the latest tar file.

The Release Notes for this offering are available at:
http://ibm.com/docs/SSWSZ5_3.2.x/rel_notes/Guardium_Insights_v3.2.0_Release_Notes.pdf

The Quick Start Guide for this offering is available at Passport Advantage (https://www.ibm.com/software/passportadvantage) (search for Part Number "M07QWML").

Installing Guardium Insights v3.2.0

Before installing Guardium Insights, review the system requirements:
http://ibm.com/docs/SSWSZ5_3.2.x/sys_req.html

This offering is deployed as a new installation of Guardium Insights – or as an in-place upgrade. Please follow these instructions:

- Prepare for installing:
  http://ibm.com/docs/SSWSZ5_3.2.x/install_prep_insights.html
- Install Guardium Insights:
  http://ibm.com/docs/SSWSZ5_3.2.x/install.html
- Upgrade process:
  http://ibm.com/docs/SSWSZ5_3.2.x/install_insights_update.html

New Features and Enhancements

Reporting

- Auditing: Guardium® Insights now offers auto-distribution, which allows you to filter audit results. This feature allows for the creation of rules that define which users receive data based on report attributes such as Client/Server IP, and database type. For example, one report can be divided up and sent to roles or individuals based on who owns the data.
- Ability to create advanced, custom filters for reports - including nested conditions, case insensitive/case sensitive, and usage of the AND/OR operators.
- In report and Not in report filters allow you to reference values in another report for correlation use cases.

Enhanced risk-based user experience

- Guardium Insights 3.2 introduces a new and enhanced risk engine. This engine replaces the now-deprecated risk analysis feature, that was based on anomalies. It connects the dots by using many data points to understand the broader story around your system's risk.
- The enhanced risk engine includes more data points for risk calculation, such as activities, outliers, user characteristics like "privileged", vulnerability assessments, classifications, exceptions, and policy violations.
- Automate responses to risk events using Response Rules.
- Enhanced user experience that provides greater drill down capabilities for understanding how risk was calculated, database users involved, detailed reports, and related risk events.
- Ability to reduce the noise by excluding non-critical assets.
- Custom Risk profiles: Ability to customize the weighted values used in risk calculations

Best practices dashboard templates

- Out-of-the-box template dashboards based on years of accumulated knowledge in the industry.
- Accelerates customers' time to value.
- Data hygiene: Proactively observe and remediate bad behavior to preserve healthy data hygiene and ultimately reduce the risk for your organization.

Universal connector

- Template universal connector plug-in that makes it easy for you to write your own universal connector plug-in.
- In Guardium Insights, check universal connector connectivity and health status in real time, or monitor connectivity and health status over a period of time.

Operational enhancements

- Ability to use Prometheus for detailed monitoring of Guardium Insights ingestion micro services.
- Data mart ingestion dashboard: End-to-end status of data mart ingestion that allows click down filtering using a timeline view. This feature includes the addition of the Data mart ingestion status report.
- The script for purging hot storage data has been improved. It now purges tables related to outliers and risk data.
- Guardium Insights can now detect outliers for data received from Guardium Data Protection as summarized data and direct streaming from either cloud sources or universal connector.

Integrations

- Guardium Insights now supports IBM Security Discover and Classify (1touch.io Inventa) and IBM Security Guardium Big Data Intelligence (GBDI) file integrations.

Bug fixes

Issue key	Description
INS-12690	Unable to apply filter to report definition. The filter panel is able to open, regardless of the amount of data. However, when you drill down to see the values of a column that has a lot of data, the drop-down bar hangs or the browser displays a timeout message.
INS-14335	If you create a group with Errors as the group type, the group is not available in reports when using error code, error cause, or exception description filters.
INS-14727	There is an issue calculating the correct hour to run after midnight for an hourly process.
INS-15806	iSeries itaps are not supported in the Guardium Data Protection health view or in the corresponding health views on GDP.
INS-15851	Unable to save alert action policies, given either of these conditions: • When using any result set with the Alert per match action. • If a rule is expanded and you click Save and activate.
INS-15945	Applications fail to connect to the Db2 database.
INS-15876	Status information is not available for unhealthy connections.
INS-16001	Some NLS keys are not being translated on the anomalies page when manually creating a ticket
INS-16010	Searching the audit results does not work as expected.
INS-16029	When creating a Guardium connection integration, when you specify a Start date, the previous day is chosen.
INS-16030	When ELB is enabled, S-TAP cannot be migrated from Guardium Data Protection to Guardium Insights.
INS-16050	If you create a PAM integration and then edit the integration, the connection fails
INS-16678	When you upload the wrong universal connector plug-in, Guardium Insights stays in a loading state, without providing any notification messages.
INS-16690	On the Central Manager page, if there is an issue with any managed units, the Central Manager associated with those managed units will have a status indicating that there is a collector issue. This can be problem because it could be only the aggregators that are having issue and thus making the status confusing and misleading.
INS-16695	When creating a schedule that starts the next day, it runs at 12 AM instead of the correct time based on the selected time zone.
INS-16697	Time zone control is not initialized with the user's preferred time zone.
INS-16700	After creating a scheduled job, privileges are not automatically refreshed.
INS-16702	You cannot add a numeric value to the filter from a chart.
INS-16767 INS-17025	Data marts from the previous day do not bring expected data from collectors.
INS-16789	When your Guardium Central Manager is upgraded to p343, but the managed unit is below p317, there is a discrepancy between old code and new data marts.
INS-16792	When editing a report through the dashboard user interface, if you select CSV Export in the report editor, you will not be able to select the option to export all of the report's rows.
INS-16798	After your GDP appliance managed unit is upgraded from a previous patch to p343, existing scheduled Guardium Insights data marts are not immediately rescheduled with

	the latest data mart set that was introduced in p343. Rather, they are updated within 24 hours, by design.
INS-16855	The Db2 schema upgrade script changes the archive log configuration, which includes temporarily disabling the Db2 network listener, restarting Db2, taking an offline backup, then enabling listener and restarting Db2 again. If this sequence fails, Db2 may be left in an inoperable state, requiring manual intervention.
INS-16884	After upgrading Guardium Insights, uploaded universal connector plug-ins are no longer available.
INS-16890	Universal connector persistent queue is not enabled by default.
INS-16923	In Settings > Global settings > Report settings, you can set a Report data retrieval timeout. If this is set to a value greater than 15 minutes, you may receive this error when running a report: Cannot retrieve the report data. Refresh the page or retry later. Unexpected token < in JSON at position 0
INS-16926	In the Scheduled and audited jobs page, searching for regular expressions (RegEx) in the Regex search field does not work.
INS-16976	Unable to see universal connector data sources when the correct plug-ins are not uploaded.
INS-17021	Editing the password (connection credential) in a connection results in “incorrect credentials message.
INS-17047	If you have connected Guardium Data Protection with patch p343 to Guardium Insights Version 3.0.2 and you upgrade to Version 3.1.0, you will not be able to click on the Aggregator tab to enable historical data export from the aggregator.
INS-17051	You receive a message indicating a failure to load group data, and the problem temporarily goes away if you refresh the screen.
INS-17074	When using a universal connector, MySQL and HDFS traffic are not monitored with the default active policy installed.
INS-19488	Db2 SORTHEAP errors when running a report in Guardium Insights.

SECURITY FIXES

Issue key	PSIRT	Vulnerability ID
INS-20804	PVR0350831	CVE-2019-10782
INS-20808	PVR0350878	CVE-2018-1000632
INS-20814	PVR0350925	CVE-2020-8908
INS-20815	PVR0350936	CVE-2019-14900 CVE-2020-25638
INS-20816	PVR0350939	X-Force 221454
INS-20817	PVR0350941	CVE-2020-13956
INS-21755	PVR0366466	n/a

Known limitations and workarounds

Guardium Insights component	Issue key	Description
Anomalies	INS-22749	Deprecated v3.1 Anomaly Rules appear enabled in v3.2 **Workaround:** These rules will not run. It is safe to delete the deprecated Anomaly Rules.
Auditing and scheduling	INS-22169 INS-22838	Existing temp tables created for scheduled audit tasks take most of the Db2 space and cause remaining scheduled jobs fail to save new temp tables. These remaining jobs will fail. **Workaround:** Go to **Settings > Global Settings > Reports** and reduce the number of days a scheduled report download file is maintained (the default is 30 days). This saves disk space and avoids failure.
	INS-22213	The search function in the scheduled job page only searches those jobs that are in the current page. If there are additional pages, they are not included in the search results. There is no workaround for this limitation.
Data source connections	INS-15167	In some cases, the number of successful SQL statements and the total count of SQL statements stored in the instance table is higher than expected (the total count includes both failed and successful SQLs). This occurs when streaming from AWS, Azure, and S-TAP. Data marts are unaffected. There is no workaround for this limitation.
Data marts	INS-18077	If the ingestion queue has 65536 or more files waiting to be ingested, the ingestion stops. **Workaround:** For all files that are sitting on the system, the `_COMPLETE` files need to be deleted and created again.
	INS-21621	Ingestion information for data marts that are received from aggregators is not displayed. There is no workaround for this limitation.
	INS-21623	If data fails to transfer with SCP in the previous hours, all of the CSV will be retrieved in a tar file with a later start time. This results in a mismatch of the counts. There is no workaround for this limitation.

	INS-22645	Some scenarios result in skipped data mart file clean-up (ingestion happens, but deletion fails). When this happens, the files remain on the cluster. There is no workaround for this limitation.
	INS-23168	If there is a bad record (for example, one that Db2 fails to parse) in the upper half of a CSV file, Db2 fails to ingest the entire file. There is no workaround for this limitation.
Guardium Data Protection health	INS-22217	If you use Guardium Insights instead of an aggregator, the GDP health dashboard shows the aggregator status as `medium`. **Workaround:** Go to the GDP Health pages (**Deployment Topology/Table/Stap** and **GIM Dashboard**) and click the customization icon. In the pop-up dialog box, remove the "aggregation" status and then wait for approximately 5 minutes in Guardium Insights to see the changes.

Installation and upgrade	INS-23116	If Db2 is being upgraded, it is possible that a race condition will occur when the `db2-ready` job checks if DB2 is up just before it shuts down for an upgrade. This causes the remainder of the script to fail silently because the Db2 client has the same exit code for situations when DB2 is down and when the entity it tries to create already exists.
		
		Workaround: Issue this command:
		`oc delete \`oc get jobs -o name | grep db2-ready\``
		To validate that the command worked, issue this command:
		`oc logs \`oc -o name get pods | grep db2-ready\` | grep -e 'A database connection does not exist' -e 'container is not created or running'`
		This command should not return any results.
		Note that it may take up to 40 minutes for the `db2-ready` pod to be created again, so an error due to missing pod name is normal.

	INS-23223	By default, the all-in-one script uses the RWX storage class for backup and restore support. This forces you to stop the deployment, update the CR, and apply it (in the case that you want to use a different RWX storage class for the backup and restore support in the deployment). **Workaround:** 1. Edit the `values.conf` file before running the all-in-one script by changing the default value of `APPLY_CR` from `true` to `false`. 2. After the script runs, locate the custom resource (CR) created by the script and then make changes as required - and then apply back the CR. **Note:** This is an optional step for deployments on AWS, Fyre, AZURE, and GCP - as the RWX storage class recommendations mentioned in the documentation can be as it is used for the backup and restore support. However, for IBM-CLOUD, this is a mandatory step because on IBM-CLOUD, `managed-nfs-storage` is required for backup and restore support (`managed-nfs-storage` needs to be configured and set up prior to the deployment).
Outliers	INS-21683	When a timeframe is displayed on an outlier table, it should be converted to the corresponding string. However, If the timeframe value is assigned any number other than 8 or 9, the table will display a non-converted value. **Workaround**: The table will display a non-converted value. If you want to avoid confusion, you can remove the timeframe column from the table.
	INS-22685	Changing the outlier feature flag does not take effect if data mart streaming is currently enabled **Workaround:** After updating the outlier feature flag, re-enable streaming from the central manager. For aggregator managed units, if aggregator export has already been completed, then set the aggregator start and end date to the current day before enabling streaming. A future patch of IBM Guardium 11.5 will not require this manual re-enablement in IBM Guardium Insights.

	INS-23311	Aggregators are not continuously streaming data when the `OUTLIERS_ENGINE` feature flag is set to `true` and showing `Data export completed`. **Workaround:** Set the end date to a date that is far in the future when setting up data export for aggregators.
	INS-23562	If you back up and then restore Guardium Insights, new outliers are not generated on the restored environment. Due to a known issue when restoring Guardium Insights, the tenant directory is deleted, but not recreated when the cluster is up and running. **Workaround:** Manually create the tenant directory (using the name of the tenant ID) in the `/mnt/blumeta0/scratch/insights-data-extraction/` path on Db2.
Policies	INS-20681	If you click on a template policy, press **Cancel**, and then reopen the window to choose a different template policy, the options (groups to select or integrations) and rules that appear will not be applicable to that specific template policy. **Workaround**: Refresh the page after pressing **Cancel** to get the correct template contents for the template policy.
Reports	INS-21619	When the API hits the time limit that is set in the Guardium Insights global settings, the API should return a timeout message rather than an error message. However, IBM Cloud has its own time limit setting. Consequently, if the Guardium Insights time limit is greater than IBM Cloud time limit, the API will throw an error message **Workaround**: In order to avoid confusion, the time limit for Guardium Insights should be set below 50 seconds, which is the IBM Cloud default time limit (see https://cloud.ibm.com/docs/vpc?topic=vpc-advanced-traffic-management#connection-timeouts). If you do this, you will see a timeout message instead of an error message.

	INS-22686	Some Guardium Insights API (for example, reports API) take longer than 60 seconds. On AWS Cloud, these API fail. For example, the report will result in this error: `Report error cannot retrieve the report data. Refresh the page or retry later. Failed to fetch` **Workaround:** Increase the timeout to be 4000 seconds instead of 60 seconds on the AWS classic load balancer 1. Log in to your AWS account and to your region 2. Go to EC2. 3. Under EC2, there is Load balancer tab. Change its idle timeout for all classic LB (type = classic) from 60 seconds to 4000 seconds.
	INS-23033	This error occurs for IBM Cloud VPC Gen 2 when running reports or when there are API timeouts: `Report error Cannot retrieve the report data. Refresh the page or retry later. NetworkError when attempting to fetch resource.` **Workaround:** Open a case with IBM Cloud support to increase the timeout for the load balancer that the IBM Cloud Openshift cluster creation creates.
Risk events	INS-22332	When opening a drilldown report from the right-side panel of a finding, it is possible to lose the last minute of data. For example, if you set the end time to 16:00:00, data after 16:00:01 will not be displayed on the table. **Workaround**: Using the same example, if you want to include data after 16:00:01, set the end time to 16:59:59 in the custom time filter.
	INS-22622 INS-22584	Linking vulnerability assessment and classification results to a database can only be done if the data source in Guardium Data Protection was defined using a server IP address. **Workaround:** Define the data source in Guardium Data Protection using a server IP address.

Universal connector	INS-20962	In `uc gi_templates.json`, there may be a nested sensitive field (credential) that cannot be updated in the edit sidebar in the connections page. **Workaround:** Put the sensitive fields in the flat level (first level) of `gi_templates.json`. Alternatively, you can delete and recreate the connection.
	INS-22167	In extreme cases when data is moving from many nodes to one, there might be data loss. This occurs even when the persistence queue is turn on. **Workaround:** Ensure that there are enough nodes available.

Resources

IBM Security Guardium Insights documentation
http://ibm.com/docs/SSWSZ5_3.2.x/

System Requirements
http://ibm.com/docs/SSWSZ5_3.2.x/sys_req.html

IBM Security Learning Academy
https://www.securitylearningacademy.com