IBM Resilient

resilient

Incident Response Platform

Release Notes V30.4

Release Date: September 2018

Introducing the next generation of incident response. Intelligent Orchestration dramatically accelerates and sharpens response by seamlessly combining incident case management, orchestration, automation, and intelligence into a single platform. The Resilient next-generation platform is the first to deliver real-time visibility across your SOC tools, quick time to value, and guided response that empowers your team to outsmart, outpace, and outmaneuver cyberattacks.

FEATURES AND ENHANCEMENTS

The V30.4 release of the Resilient Incident Response Platform introduces a number of new features and enhancements. All changes and bug fixes from the previous V30 releases (V30.0, V30.1, V30.2, and V30.3) are included.

The following new features and enhancements are provided in V30.4:

- **Incident History Detail Report:** It is now possible to download a report of the incident history formatted as a Microsoft Excel spreadsheet. This format is a much more efficient and effective way to view incident history for incidents with a very large volume of changes. The report is generated on the server and can be downloaded to the browser when the report is complete. The end user is notified when the report is ready to download.
- **Change to client access log:** For on-premises customers only. The client access log now contains two entries for each request. The first entry logs the request initiation. The second entry logs the request completion. This enhancement can be particularly helpful when troubleshooting issues (for example, issues with proxy servers). Previously, only completed requests were logged.

- **Privacy**: The following changes have been made to the Privacy Module in this release:
    - All Canadian regulators have been moved from the Record Count page to the Regulators page.
    - Existing Canadian special regulators have been renamed and moved to a subsection.
    - The following U.S. States & Territories have been updated:
        - Colorado
        - Nebraska
    - The following new regulators have been added:
        - Canada Special Regulators: Alberta (Health)
        - Europe: Gibraltar
        - Europe: Guernsey
        - Europe: Isle of Man
        - Europe: Jersey
    - The following new data types have been added:
        - Identification Data: Student ID Number
    - The GDPR Breach Risk Assessment has been changed as follows:
        - The section has been renamed to Europe Breach Risk Assessment.
        - The associated condition has been updated to replace the individual regulator values with a single new generic value. The new value applies to all regulators that are defined as Breach Risk Assessment Regulators. Therefore, if the list of Breach Risk Assessment Regulators is changed, the condition automatically triggers the risk assessment accordingly.

Updating Privacy rules

This release includes new European regulators (Gibraltar, Guernsey, Isle of Man, and Jersey). The Europe Breach Risk Assessment (formerly labelled GDPR) has been updated to use a new generic condition to determine the associated regulators, including these new regulators.

For new installations of Resilient V30.4, the new generic breach risk assessment condition is automatically applied, and risk assessment for these new regulators is automatically triggered.

For existing Resilient installations, if you want to apply these changes, you must manually update the New Incident Wizard layout and the incident Breach tab layout. If you already updated your layouts to apply the GDPR functionality in a previous version of Resilient, you must make additional minor modifications. For instructions on how to apply the latest changes, see GDPR updates for Resilient V30.4 (September 2018).

Audit Logging Considerations

If you enabled audit logging in V30.2 or V30.3, you must restart auditing after you upgrade to V30.4 to ensure that your system continues to log data correctly.

Complete the following steps:

1. Check whether auditing is enabled:

   ```
   sudo ls -l /usr/share/co3/conf/logback-audit.xml
   ```

   If the `logback-audit.xml` file does not exist, audit logging is not enabled. No further action is necessary.

2. If the `logback-audit.xml` file is present, audit logging is enabled. Restart auditing as follows:

   ```
   sudo resutil audit -off
   Command successful. The Audit Logging configuration is as follows
   Status: Off
   ```

   ```
   sudo resutil audit -on [ -port <num> ]
   Command successful. The Audit Logging configuration is as follows
   Status: On    Type : yslog    Host : localhost    Port : 514
   ```

3. One or more temporary log files (`client.log*.tmp`) might be created in the `/usr/share/co3/logs` directory by the audit restart. Archive these files, as described in the next section.

For more information about audit logging, see the Installation Guide.

Temporary log files

One or more temporary log files (`client.log*.tmp` or `monitoring.log*.tmp`) might be created occasionally in the `/usr/share/co3/logs` directory. These files should not be deleted, because they might contain data that was not successfully archived.

Archive the temporary files, as follows.

1. Check whether any `.tmp` files exist:

   ```
   sudo bash -c "ls -l /usr/share/co3/logs/client.log*.tmp && echo 'client.log tmp files exist' || echo 'client.log tmp files do not exist'"
   ```

   ```
   sudo bash -c "ls -l /usr/share/co3/logs/monitoring.log*.tmp && echo 'monitoring.log tmp files exist' || echo 'monitoring.log tmp files do not exist'"
   ```

   If no `.tmp` files exist, no further action is necessary.

2. If `.tmp` files exist, compress the files and move them to the `daily` subdirectory:

   ```
   sudo bash -c "cd /usr/share/co3/logs; gzip client.log*.tmp; mv client.log*.tmp.gz daily"
   ```

   ```
   sudo bash -c "cd /usr/share/co3/logs; gzip monitoring.log*.tmp; mv monitoring.log*.tmp.gz daily"
   ```

   Note: The `.tmp.gz` files do not affect the logback rollover limit that is configured in the `/usr/share/co3/conf/logback.xml` file, and are not automatically deleted when the limit is reached. You should manually delete the `.tmp.gz` files when they are no longer needed, as specified by your retention policy for files in the `daily` subdirectory.

CORRECTED ISSUES

Tracking Code	Issue
RES-9115	Incident description text area does not wrap words correctly.
RES-9175	Search results show an incident to have an unassigned owner when owned by a group.
RES-9872	New incidents cannot be created if the new incident wizard contains the "Members" field.
RES-10148	Hyperlinks are stripped out of tasks.
RES-10153	Cannot delete an incident if it has running workflows with running child workflows.
RES-10404	Resilient scripting service startup timeout should be 120 seconds.
RES-10586	After upgrading to V30.3, any emails, such as notifications, in a pending state are not sent.