IBM Resilient

Incident Response Platform API

API Release Notes v30

Release Date: April 2018

Based on a knowledge base of incident response best practices, industry standard frameworks, and regulatory requirements, the Resilient Incident Response Platform helps make incident response efficient and compliant.

These release notes describe the changes to the REST endpoints and Data Transfer Objects (DTOs) in the IBM Resilient V30 API.

Features and Enhancements

The Resilient Platform V30 includes the following new features and enhancements:

- **Functions:** A *function* is a new object for invoking remote code, which performs an activity and then returns the results to the function. Functions are designed to improve the ease of building integrations with other security systems. See FunctionREST.
- **Wiki:** Users can create and edit wiki pages from within the Resilient platform. See WikiREST.
- **Workspaces:** Act as containers or partitions for grouping different incidents, and enable organizations to manage incidents more efficiently across multiple teams. Role based access control has changed as a result of this new feature. See WorkspaceREST.
- **Deprecations:** Many old deprecations have been removed.

More details are included in the general release notes, the System Administrator Guide, the Playbook Designer Guide, and the User Guide.

New REST Endpoints

The following REST endpoints have been added:

- **FunctionREST**
    - Manages functions.
- **WikiREST**
    - Manages wiki pages.
- **WorkspaceREST**
    - Manages workspaces for an organization.

Modified REST Endpoints

The following REST endpoints have been modified:

- **IncidentArtifactREST**
    - The **{artifact_id}/whois : GET** method has been removed. Use {artifact_id}/whois : POST instead.
- **IncidentREST**
    - The **{inc_id}/related : GET** method has been removed. Use {inc_id}/related_ex instead.
- **TaskREST**
    - The **delete : PUT** method has been added to facilitate deleting tasks in bulk.

Deleted REST Endpoints

The following REST endpoints have been deleted:

- **SearchREST**
    - Deprecated in v28. Use SearchExREST instead.

New DTOs

The following DTOs have been created:

- **AcknowledgementDTO**: Sent to indicate an acknowledgement by a client that is processing messages on a message destination. Replaces ActionAcknowledgementDTO. The **variables** field has been deprecated.
- **AuthorizedInstanceDTO**: Stores an instance of an object along with the roles and effective permissions associated with the object.
- **FieldDefTextTemplateDTO**: Represents a string template for a field definition. Only textarea fields without richtext can contain string templates. These templates are only applicable to function fields, not incident fields.
- **FunctionConfigurationDTO**: Stores configuration data for a function within a workflow.

- **FunctionDataDTO**: Stores information sent to a message destination when a function is executed.
- **FunctionDTO**: Represents a function.
- **FunctionInputDTO**: Stores the information about a function input binding in a FunctionConfigurationDTO.
- **MentionedWidgetDTO**: Represents a widget and its parameters.
- **ScriptConditionDTO**: Stores the information necessary to evaluate a script condition.
- **ScriptMetadataInputDTO**: Stores parameters used to retrieve metadata for the in-workflow script editor. Not used by any public endpoints.
- **StaticFunctionInputDTO**: Stores the information necessary for a static function input.
- **WikiEntryDTO**: Represents the basic information of a wiki page.
- **WikiPageDTO**: Represents a wiki page.
- **WikiPagePermsDTO**: Represents the permissions the current user has for a given wiki page.
- **WorkspaceDTO**: Stores the details of a workspace.

New Types

The following types have been added:

- **FunctionInputType**: Possible types for a FunctionInputDTO.
- **ScriptMetadataType**: Possible types of Script Metadata that can be requested. Used only in internal APIs.

Modified DTOs

The following DTOs have been modified:

- **ActionInvocationDTO**
    - The **function** field has been added to indicate information about the function invoked.
- **ConfigurationExportDTO**
    - The **functions** field has been added to contain the functions being exported from the system.
    - The **workspaces** field has been added to contain the workspaces being exported from the system.
- **ConstDTO**:
    - The **artifact_types** field has been removed. It was deprecated in v28. Use FullOrgDTO.incident_artifact_types instead.
    - The **min_session_timeout** field has been added to display the minimum time in seconds that can be set for the session timeout.

- The **max_session_timeout** field has been added to display the maximum time in seconds that can be set for the session timeout.

- **FieldDefDTO**:
  - The **default_chosen_by_server** field has been added to indicate whether the field value will be filled in by the server if it is not provided.
  - The **templates** field has been added to store an array of text templates (FieldDefTextTemplateDTOs). Only applicable for text fields.
- **FullIncidentDataDTO**:
  - The new **workspace** field is inherited from IncidentDTO.
- **FullOrgDTO**
  - The **artifact_types** field has been removed. It was deprecated in v28. Use incident_artifact_types instead.
- **FullUserDTO**
  - FullUserDTO inherits the changes made in UserDTO.
- **GroupDTO**
  - The **role_handles** field has been deprecated. Use instance_roles instead.
  - The **instance_roles** field has been added to show the group's authorization information.
- **IncidentDTO**:
  - The **workspace** field has been added to display the incident's workspace.
- **IncidentPermsDTO**:
  - The **change_workspace** field has been added to show whether the user can change the workspace of the incident.
- **NewsfeedEntryDTO**:
  - The **user** field has been deprecated. Use the principal field instead.
  - The **principal** field has been added to show the user information.
- **NotificationDTO**:
  - The **inc_id, inc_training, inc_name, task_name, task_id, comment_text,** and **comment_id** fields have been removed. They were deprecated in version 28. See notification_text instead.
- **SessionOrgInfoDTO**
  - The **effective_permissions** field has been deprecated. Use AuthorizedInstanceDTO.effective_permissions instead.
  - The **role_handles** field has been deprecated. Use AuthorizedInstanceDTO.role_handles instead.

    - The **instance_roles** field has been added to show the user's authorization information.

- **TaskDTO**:
    - The **auto_task_id** field has been removed. It was deprecated in v27. Use at_id instead.

- **UserDTO**
    - The **role_handles** field has been deprecated. Use instance_roles instead.
    - The **instance_roles** field has been added to show the user's authorization information.

- **UserOrgDTO**
    - The **role_handles** field has been deprecated. Use instance_roles instead.
    - The **instance_roles** field has been added to show the user's authorization information.

- **WorkflowDTO**:
    - The **actions** field has been added to show the actions that reference this workflow.

Modified Types

The following types have been modified:

- **MethodName**:
    - **script** has been added as a value.

- **TypeId**:
    - **function** and **workspace** have been added as values.

Deprecated DTOs

The following DTOs are deprecated in this release:

- **ActionAcknowledgementDTO**: Use AcknowledgementDTO instead.

Deleted DTOs

The following deprecated DTOs have been deleted in this release:

- **CategorySearchResultDTO**: Removed as a part of the removal of SearchREST. Deprecated in v28.
- **IncidentArtifactResultDTO**: Removed as a part of the removal of SearchREST. Deprecated in v28.
- **IncidentCommentDTO**: Use CommentDTO instead. Deprecated in v27.2.
- **IncidentResultDTO**: Removed as a part of the removal of SearchREST. Deprecated in v28.

- **OrgIncidentArtifactTypeDTO**: Use IncidentArtifactTypeDTO instead. Deprecated in v28.
- **SearchInputDTO**: Removed as a part of the removal of SearchREST. Deprecated in v28.
- **TaskCommentDTO**: Use CommentDTO instead. Deprecated in v27.2.