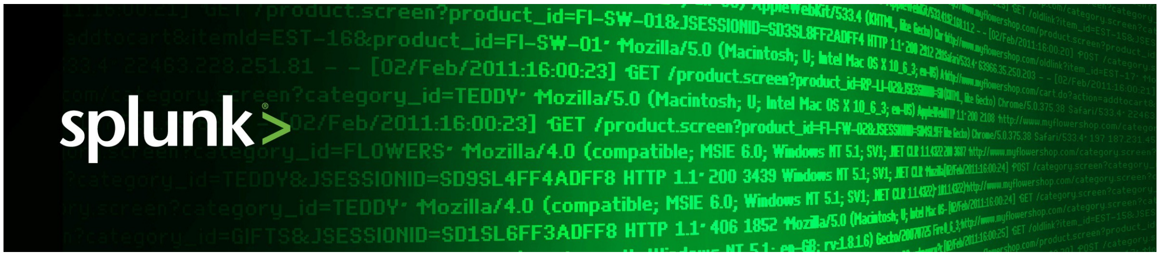

Splunk® Supported Add-ons Splunk Add-on for ServiceNow released

Configure inputs for the Splunk Add-on for ServiceNow

Generated: 4/25/2018 2:30 am

Copyright (c) 2018 Splunk Inc. All Rights Reserved

Configure inputs for the Splunk Add-on for ServiceNow

Configure data inputs to collect data from your ServiceNow instance. You can configure these inputs either by using Splunk Web or by editing `local/inputs.conf`.

In a distributed environment, configure your data inputs on a data collection node, usually a heavy forwarder.

Configure inputs using Splunk Web

1. On your data collection node, click **Settings > Data Inputs**.
2. Click on **Splunk Add-on for ServiceNow**.
3. Review the source types table, and click **Enable** under **Status** to enable the preconfigured databases you want to use.
4. (Optional) To add a ServiceNow table for data collection, click **New** and fill in the required fields.

Field name	Description
Database table name	The database table name in ServiceNow.
Collection interval	How long the Splunk platform waits before collecting data from the table, in seconds.
Excluded properties	Excluded properties of the database table, in a comma-separated list.
Time field of the table	The time field to use for checkpoint creation. The add-on creates a checkpoint for this field each time that it calls the REST API to get data, so each time the data collection resumes from the timestamp where it left off. The default is `sys_updated_on`.
Date started from	The date that the Splunk software starts collecting data from the database table, in UTC "YYYY-MM-DD hh:mm:ss" format. Default is one year ago. This configuration overrides the configuration in the setup page.
ID field	The ID of the row. The default is `sys_id`.
Filter parameters	Provide filters in key-value pairs for indexing only selected data from the table. For example, key1=value1&key2=value2. The default is no filter.

Host	The host that the Splunk software assigns to the events collected from this input.
Index	The index in which the Splunk software stores the events collected from this input. The default is `main`.

5. Click Save.

Note: If you access **Settings > Data Inputs** from anywhere other than the setup screen for the Splunk Add-on for ServiceNow, manually update the URL in your browser to change the app context to `Splunk_TA_snow`, so that the Splunk platform stores your local input configurations in your app rather than in Search or Launcher.

The CMDB table is the core ServiceNow database table. The CMDB table is a parent table that is inherited by many other tables, and enabling its data input would index records of all of its child tables. These child tables may contain more fields than its' parent table, so enabling the data input for CMDB table and any of its child tables would result in duplicate records.

Configure inputs using inputs.conf

1. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_snow/local/` and create an `inputs.conf` file.
2. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_snow/default/inputs.conf` and review the pre-configured input stanzas. Each stanza describes the data collection for one database table. By default, all inputs are disabled.
3. Copy all input stanzas relevant to your deployment to `$SPLUNK_HOME/etc/apps/Splunk_TA_snow/local/inputs.conf`.
4. To enable all the preconfigured database table inputs (recommended), change `disabled = true` to `disabled = false` in the `[snow]` stanza. This enables all the inputs in all stanzas prefixed with `snow://`.
5. To enable only certain database table inputs, leave the line `disabled = true` in the `[snow]` global stanza unchanged and add `disabled = false` to the stanzas you want to enable.
   For example, if you want to collect data from the `incident`, `change`, and `em_event` ServiceNow database tables, the corresponding `local/inputs.conf` appears as follows:

   ```
   [snow://incident]
   exclude = description
   disabled = false
   ```

```
[snow://problem]
exclude = description
disabled = false

[snow://em_event]
timefield = time_of_event
disabled = false
```

6. To configure a custom index for your data, change `index = main` to specify a different index.
7. (Optional) Configure the collection interval (`duration=`), excluded properties (`exclude=`), database table rising column (`timefield=`), and date started from (`since_when=`) for each table stanza.
8. If you want to add a new table for data collection, follow this schema to add a new stanza in `local/inputs.conf`.

```
    [snow://<servicenow_database_table_name>]
    exclude = <exclude properties of the table, in a
comma-separated list>
    duration = <collection interval for this table, in seconds>
    timefield = <the time field to use for checkpoint creation>
    since_when = <data starts from this point of time in the
table>
    id_field = <Field which uniquely identifies each row in this
table>
    filter_data = <Provide filters in key-value pairs as shown in
example for indexing only selected data from the table e.g.
key1=value1&key2=value2>
```

9. Save your changes.
10. Restart your data collection node.

The CMDB table is the core ServiceNow database table. The CMDB table is a parent table that is inherited by many other tables, and enabling its data input would index records of all of its child tables. These child tables may contain more fields than its' parent table, so enabling the data input for CMDB table and any of its child tables would result in duplicate records.