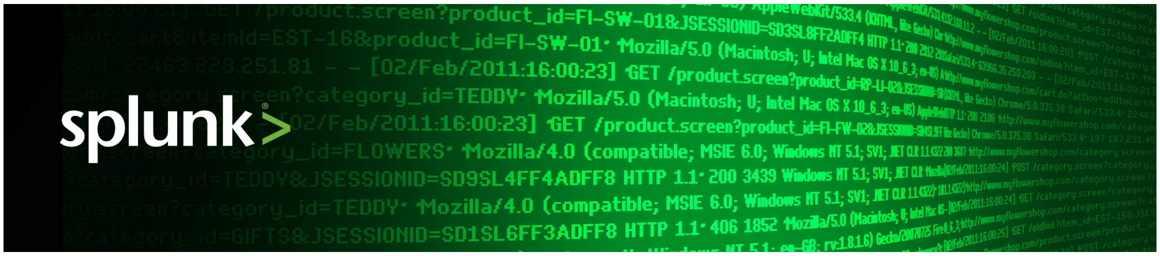

Splunk® Supported Add-ons Splunk Add-on for ServiceNow released

Troubleshoot the Splunk Add-on for ServiceNow

Generated: 5/23/2018 2:47 am

Troubleshoot the Splunk Add-on for ServiceNow

General troubleshooting

For troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in *Splunk Add-ons*. For additional resources, see Support and resource links for add-ons in *Splunk Add-ons*.

Cannot launch add-on

This add-on does not have views and is not intended to be visible in Splunk Web. If you are trying to launch or load views for this add-on and you are experiencing results you do not expect, turn off visibility for the add-on.

For more details about add-on visibility and instructions for turning visibility off, see the *Check if the add-on is intended to be visible or not* section of the Splunk Add-ons Troubleshooting topic.

Cannot access setup page

If you are trying to reach the setup page but cannot see a link to it on your instance:

1. Confirm that you are signed in with an account that is a member of the admin or sc_admin role.
2. If you are on a search head cluster, click **Settings > Show All Settings**, then follow the standard setup directions.
3. If you are on a managed Splunk Cloud version 6.6.X, access the setup page by going directly to the URL in your browser: <yourSplunkCloudURL>/manager/Splunk_TA_snow/apps/local/Splunk_TA_snow/setup?act

Find relevant errors

Search for the following event types to find errors relevant to the Splunk Add-on for ServiceNow.

Search `eventtype=snow_ta_log_error` for errors related to the add-on.

Search `eventtype=snow_ta_collector_error` for errors related to data collection from ServiceNow.

Search `eventtype=snow_setup_error` for errors related to the setup configuration.

Search `eventtype=snow_ticket_error` for errors related to creating events or incidents in ServiceNow from the Splunk platform.

Search `eventtype=ta_frwk_error` for errors related to low-level functions of the add-on.

Missing data

If you are not getting data from all of the inputs that you have enabled, check that the ServiceNow account that you are using to connect to your ServiceNow instance from the Splunk platform has, at minimum, read-only access to all of the database tables from which you are attempting to collect data. Then, disable and re-enable the inputs for which you are not receiving data.

To validate that you do not have a permissions issue:

1. Edit the following URL to use your ServiceNow instance name:

```
https://<myservicenowinstance>.service-now.com/<service_now_table>.do?JSONv2&sysparm_qu
<myservicenowinstance>.service-now.com
```

1. Change `service_now_table` to the ServiceNow table you are trying to query
2. Change `2016-01-01` to the actual date you want to query from.
3. Paste the URL into a browser.
4. When prompted, log in with the same username and password that you use for the integration account in the add-on.

If you receive the historical data you expect and a `sys_updated_on` field for each event, you have the correct permissions.

SSL certificate issue

If you encounter a `SSLHandshakeError`, the SSL certificate entry might be missing from your operating system's certificate store. Resolve the issue by adding the certificate to your operating system's trust list.

1. Navigate to the certificate store for your operating system. Certificate store locations vary by operating system.
2. Add the SSL certificate.
3. Save your changes.

By default, the SSL handshake is configured to function normally. The certificate used by ServiceNow is signed by the Entrust Certification Authority.

For more information on adding SSL certificates to your operating system's certificate store, see the How can I trust CAcert's root certificate? page in the CAcert Certificate Authority wiki.

Turn off SSL certificate communication

Communication to ServiceNow is performed via HTTPS. SSL certificate validation is enabled by default. You can turn off SSL certificate validation:

1. Navigate to `$SPLUNK_HOME/Splunk_TA_snow/local/`, and create a `service_now.conf` file if it does not already exist.
2. Open the `service_now.conf` file, and add `disable_ssl_certificate_validation = 1` to the `snow_default` stanza, as shown below:

   ```
   [snow_default]
   disable_ssl_certificate_validation = 1
   ```
3. Save your changes.

Custom search commands or alert-triggered scripts fail with no results

Check that you have successfully integrated your ServiceNow instance with your Splunk platform instances. If the configuration is unsuccessful, your searches will return "No results found" and the Splunk software logs a `u_splunk_incident does not exist` error, which you can find by searching for `eventtype=snow_ticket_error`.

If your integration is successful, but incident and event creation fails, run the search `"eventtype=snow_ticket_error"` to see what errors are reported. If the failure reason is error code 302, review the ServiceNow URL that you entered in the Setup page to make sure it is correct and does not end with any special characters or trailing slashes.

See Configure ServiceNow to integrate with the Splunk platform to learn more

Errors for data collection for specific database tables

If you are missing data for a specific database table, check your `splunk_ta_snow_main.log`.

"Fail to connect...... Not Found", means that the database table has no records.

"Fail to connect ...... bad request", means that ServiceNow is reporting that that database table does not exist.

Missing fields after upgrading to Splunk Add-on for ServiceNow 3.0.0

If you have ServiceNow data indexed into your Splunk instance after upgrading to Splunk Add-on for ServiceNow 3.0.0 from an earlier version, the following panels in the Splunk App for ServiceNow do not display the existing data correctly. Any newly indexed data is not impacted.

- **Change Ticket Lookup** under **cmdb**
- **Incident Ticket Lookup** under **cmdb**
- **Incident Count by Location** under **Incidents > Open Incidents by Geography**

If fields are missing or new fields start with "dv" after upgrading, see Upgrade the Splunk Add-on for ServiceNow.

Remove deleted configuration items from the configuration management database lookups

Service Now API for configuration management database (CMDB) does not tell you what configuration items (CI) have been deleted from CMDB. As a result, Splunk does not remove CIs from the CMDB lookups that are deleted. You can manually delete the CIs from the CMDB:

1. Enable the data collection for `sys_audit_delete`:
    1. Click **Settings -> Data inputs**.
    2. Select **Splunk Add-on for ServiceNow**.
    3. Enable the sys_audit_delete data input
2. Create a saved search:
    1. Create a saved search with the name "ServiceNow Sys Delete List"

```
sourcetype="snow:sys_audit_delete" | stats count by
tablename,documentkey | rename documentkey as sys_id
```

1.
    1. Set the `Earliest` as 0 and `Latest` as now.
    2. Check the **Accelerate this search** check box and select **All Time** as **Summary Range**.
    3. Save the search.

    4. Set the saved search to **Global**.

2. After creating the saved search, update the existing savedsearch. This change should match the lookup ids with the `sys_audit_delete` table ids and remove it from the lookup. Update the saved search of cmdb tables. In this example, the saved search is named "ServiceNow CMDB CI Server":

```
eventtype=snow_cmdb_ci_server | dedup sys_id | fields - _bkt,
_cd,_indextime,_kv,_raw,_serial,_si,_sourcetype,_subsecond, punct,
index, source, sourcetype  | inputlookup append=t cmdb_ci_server_lookup
| dedup sys_id | outputlookup cmdb_ci_server_lookup
```

Add the following to each query:

```
| join max=0 type=left sys_id [ | savedsearch "ServiceNow Sys Delete
List" | eval sys_id_delete=sys_id | table sys_id,sys_id_delete ]  |
where isnull(sys_id_delete)
```

Modified query:

```
eventtype=snow_cmdb_ci_server | dedup sys_id | fields - _bkt,
_cd,_indextime,_kv,_raw,_serial,_si,_sourcetype,_subsecond, punct,
index, source, sourcetype  | join max=0 type=left sys_id [ | savedsearch
"ServiceNow Sys Delete List" | eval sys_id_delete=sys_id | table
sys_id,sys_id_delete ]  | where isnull(sys_id_delete) | dedup sys_id |
outputlookup cmdb_ci_server_lookup
```

Repeat this procedure for each of the following saved searches:

- ServiceNow CMDB CI List
- ServiceNow CMDB CI Server
- ServiceNow CMDB CI VM
- ServiceNow CMDB CI Infra Services
- ServiceNow CMDB CI Database Instances
- ServiceNow CMDB CI App Servers
- ServiceNow CMDB CI Relation
- ServiceNow CMDB CI Services