

View your event collections in Splunk

Krypton

After setting up your bulk or dynamic share within your ServiceNow sharing instance, ServiceNow data will be collected into Splunk's HTTP Event Collector. Event Collections can be filtered by source type if multiple data sources were configured when [generating your Splunk Event Collector token](#).

Prerequisites

- ⚠ You will first need to [create a ServiceNow bulk/dynamic share for Splunk](#).
- ⚠ You will also need to [point your Splunk HTTP Event Collector port to the Perspectium Integration Mesh](#) and [generate a Splunk Event Collector token](#).

Procedure

To view your event collections in Splunk, follow these steps:

1

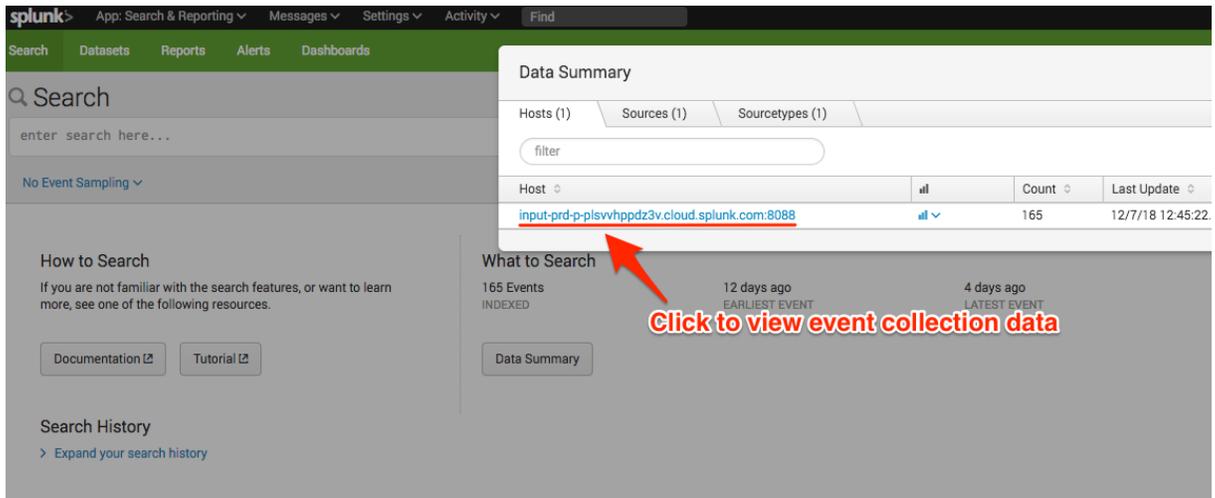
After executing your bulk share for Splunk or creating your dynamic share for Splunk and creating/updating/deleting records, log into your Splunk instance and click the Splunk logo to navigate to your instance's homepage.

2

From the left side navigation menu, click **Search and Reporting**.

3

On the resulting page, click the **Data Summary** button under **What to Search**. Then, click your Splunk instance name under **Host**.



The screenshot shows the Splunk Search interface. A 'Data Summary' modal is open, displaying a table of hosts. The table has columns for 'Host', 'Count', and 'Last Update'. The host 'input-prd-p-plsvhpdz3v.cloud.splunk.com:8088' is highlighted, with a red arrow pointing to the 'Data Summary' button in the 'What to Search' section below the table. The 'What to Search' section also shows '165 Events INDEXED', '12 days ago EARLIEST EVENT', and '4 days ago LATEST EVENT'. A red text overlay says 'Click to view event collection data'.

Host	Count	Last Update
input-prd-p-plsvhpdz3v.cloud.splunk.com:8088	165	12/7/18 12:45:22

4

Your event collection data will appear on the resulting page.

1 sourcetype="perspectium"

✓ 33 events (12/5/19 8:00:00.000 PM to 12/6/19 8:17:02.000 PM) No Event Sampling

Events (33) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 20 Per Page

Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS # active 1 # approval 1 # category 1 # incident_state 1 # number 11				
INTERESTING FIELDS # child_incidents 1 # escalation 1 # eventtype 1 # host 1 # impact 2 # index 1 # knowledge 1 # linecount 1 # made_sla 1 # notify 1 # opened_at 11 # priority 2 # punct 3 # reassignment_count 1 # reopen_count 1 # severity 1 # short_description 9 # source 1				
		>	12/6/19 8:15:54.000 PM	incident.bulk active = true : approval = not requested : category = inquiry : incident_state = 1 : number = INCO010936
		>	12/6/19 1:26:31.000 AM	incident.bulk active = true : approval = not requested : category = inquiry : incident_state = 1 : number = INCO010045
		>	12/6/19 1:26:31.000 AM	incident.bulk active = true : approval = not requested : category = inquiry : incident_state = 1 : number = INCO010010
		>	12/6/19 1:26:31.000 AM	incident.bulk active = true : approval = not requested : category = inquiry : incident_state = 1 : number = INCO010079
		>	12/6/19 1:26:31.000 AM	incident.bulk active = true : approval = not requested : category = inquiry : incident_state = 1 : number = INCO010074
		>	12/6/19 1:26:31.000 AM	incident.bulk active = true : approval = not requested : category = inquiry : incident_state = 1 : number = INCO010078
		>	12/6/19 1:20:56.000 AM	{ [-] active: true approval: not requested category: inquiry child_incidents: 0 escalation: 0 impact: 3 incident_state: 1 knowledge: false

If no data appears or if you want to view data for a specific time/date range, click the **Last 24 hours** dropdown at the top right-hand corner of the form to change the time range for which your event collection data will be displayed.

splunk> App: Search & Reporting Messages Settings Activity Find

Search Datasets Reports Alerts Dashboards Search

New Search Save As Ne

host="input-prd-p-1svvhppdz3v.cloud.splunk.com:8088" **Click to change event data time range** Last 24

✓ 0 events (12/9/18 10:00:00.000 PM to 12/10/18 10:21:48.000 PM) No Event Sampling

Events (0) Patterns Statistics Visualization

⚠ No results found. Try expanding the time range.

Presets

Real-time	Relative	Other
30 second window	Today	All time
1 minute window	Week to date	Last 15 minutes
5 minute window	Business week to date	Last 60 minutes
30 minute window	Month to date	Last 4 hours
1 hour window	Year to date	Last 24 hours
All time (real-time)	Yesterday	Last 7 days
	Previous week	Last 30 days
	Previous business week	
	Previous month	
	Previous year	

> Relative

> Real-time

> Date Range

> Date & Time Range

> Advanced

By default, data is saved into Splunk where the event name is the **name** field of the outbound message such as **incident.bulk** and the fields of the shared record are saved as fields in the Splunk event:

10/16/19 8:52:22.000 PM incident.bulk

Event Actions ▾

Type	Field	Value
Selected	<input checked="" type="checkbox"/> source ▾	httpServiceNow
	<input checked="" type="checkbox"/> sourcetype ▾	perspectium
Event	<input type="checkbox"/> active ▾	true
	<input type="checkbox"/> approval ▾	not requested
	<input type="checkbox"/> category ▾	inquiry
	<input type="checkbox"/> child_incidents ▾	0
	<input type="checkbox"/> dv_approval ▾	Not Yet Requested
	<input type="checkbox"/> dv_category ▾	Inquiry / Help
	<input type="checkbox"/> dv_escalation ▾	Normal
	<input type="checkbox"/> dv_impact ▾	3 - Low
	<input type="checkbox"/> dv_incident_state ▾	New
	<input type="checkbox"/> dv_notify ▾	Do Not Notify
	<input type="checkbox"/> dv_opened_by ▾	System Administrator
	<input type="checkbox"/> dv_priority ▾	5 - Planning
	<input type="checkbox"/> dv_severity ▾	3 - Low
	<input type="checkbox"/> dv_state ▾	New
	<input type="checkbox"/> dv_sys_class_name ▾	Incident
	<input type="checkbox"/> dv_sys_domain ▾	global
	<input type="checkbox"/> dv_upon_approval ▾	Proceed to Next Task
	<input type="checkbox"/> dv_upon_reject ▾	Cancel all future Tasks
	<input type="checkbox"/> dv_urgency ▾	3 - Low
	<input type="checkbox"/> escalation ▾	0
	<input type="checkbox"/> eventtype ▾	sourcetype=perspectium
	<input type="checkbox"/> impact ▾	3
	<input type="checkbox"/> incident_state ▾	1

But data can also be saved such that all the record's fields are saved in the Event name instead:

```
> 5/13/20 11:26:40.000 PM { "active": "true", "approval": "not requested", "category": "inquiry", "child_incidents": "0", "escalation": "0", "impact": "3", "incident": "1", "knowledge": "false", "made_sla": "true", "notify": "1", "number": "INC0047400", "opened_at": "2019-09-16 23:36:52", "priority": "5", "reopened_count": "0", "reopen_count": "0", "severity": "3", "short_description": "PannyFanny Test Incident: 37399", "state": "1", "sys_class_name": "Incident", "sys_created_by": "admin", "sys_created_on": "2019-09-16 23:36:52", "sys_domain": "global", "sys_domain_path": "\\", "sys_id": "0199aa8733cc4bc8de", "sys_mod_count": "0", "sys_updated_by": "admin", "sys_updated_on": "2019-09-16 23:36:52", "upon_approval": "proceed to next task", "urgency": "3", "dv_upon_reject": "Cancel all future Tasks", "dv_opened_by": "System Administrator", "dv_sys_domain": "global", "dv_state": "New", "dv_impact": "3 - Low", "dv_priority": "5 - Planning", "dv_notify": "Do Not Notify", "dv_sys_class_name": "Incident", "dv_severity": "3 - Low", "dv_urgency": "3 - Low", "dv_state": "New", "dv_sys_class_name": "Incident", "dv_sys_domain": "global", "dv_upon_approval": "Proceed to Next Task", "dv_category": "Inquiry \\/ Help" }
```

Show syntax highlighted

active = true | approval = not requested | category = inquiry | incident_state = 1 | index = summary | number = INC0047400

To save data in this format, update the Splunk meshlet's configuration file to have the **saveInEvent** configuration as true:

```
perspectium:
  message:
    saveInEvent: true
```

Contact support@perspectium.com if you have any questions on updating this and other configurations.

(Optional) Next steps

[Enable indexer acknowledgement](#)