

# 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 Perspective 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 & Reporting interface. The left sidebar contains navigation links: Search, Datasets, Reports, Alerts, and Dashboards. The main content area is divided into sections: 'Search' with a search bar, 'How to Search' with links to Documentation and Tutorial, and 'Search History' with a link to Expand your search history. The 'What to Search' section is active, displaying a 'Data Summary' panel. This panel has tabs for Hosts (1), Sources (1), and Sourcetypes (1). Below the tabs is a filter input field. A table lists the data sources with columns for Host, Count, and Last Update. The first entry is 'input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088' with a count of 165 and a last update of 12/7/18 12:45:22. A red arrow points to this entry with the text 'Click to view event collection data'.

Host	Count	Last Update
input-prd-p-plsvvhppdz3v.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"	Las
✓ 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 ▾ < Prev		
< Hide Fields	All Fields	
SELECTED FIELDS		
a active 1		
a approval 1		
a category 1		
# incident_state 1		
a number 11		
INTERESTING FIELDS		
# child_incidents 1		
a escalation 1		
a eventtype 1		
a host 1		
# impact 2		
a index 1		
a knowledge 1		
# linecount 1		
a made_sla 1		
# notify 1		
a opened_at 11		
# priority 2		
a punct 3		
# reassignment_count 1		
# reopen_count 1		
# severity 1		
a short_description 9		
a source 1		
i	Time	Event
>	12/6/19 8:15:54.000 PM	incident.bulk active = true approval = not requested category = inquiry incident_state = 1 number = INC0010936
>	12/6/19 1:26:31.000 AM	incident.bulk active = true approval = not requested category = inquiry incident_state = 1 number = INC0010045
>	12/6/19 1:26:31.000 AM	incident.bulk active = true approval = not requested category = inquiry incident_state = 1 number = INC0010010
>	12/6/19 1:26:31.000 AM	incident.bulk active = true approval = not requested category = inquiry incident_state = 1 number = INC0010079
>	12/6/19 1:26:31.000 AM	incident.bulk active = true approval = not requested category = inquiry incident_state = 1 number = INC0010074
>	12/6/19 1:26:31.000 AM	incident.bulk active = true approval = not requested category = inquiry incident_state = 1 number = INC0010078
>	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-plsvvhppdz3v.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 ▾

Presets

Real-time

30 second window

1 minute window

5 minute window

30 minute window

1 hour window

All time (real-time)

Relative

Today

Week to date

Business week to date

Month to date

Year to date

Yesterday

Previous week

Previous business week

Previous month

Previous year

Last 15 minutes

Last 60 minutes

Last 4 hours

Last 24 hours

Last 7 days

Last 30 days

Other

All time

> Relative

> Real-time

> Date Range

> Date & Time Range

> Advanced

No results found. Try expanding the time range.

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	http:ServiceNow
	<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_state": "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": "0199aa8733cc4bcbde",
  "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_sys_domain": "global",
  "dv_state": "New",
  "dv_urgency": "3 - Low",
  "dv_severity": "3 - Low",
  "dv_approval": "Not Yet Requested",
  "dv_escalation": "Normal",
  "dv_upon_reject": "Cancel all future Tasks",
  "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](mailto:support@perspectium.com) if you have any questions on updating this and other configurations.

## (Optional) Next steps

[Enable indexer acknowledgement](#)