View your event collections in Splunk

Gold

After setting up your bulk or dynamic share within your SeviceNow 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.

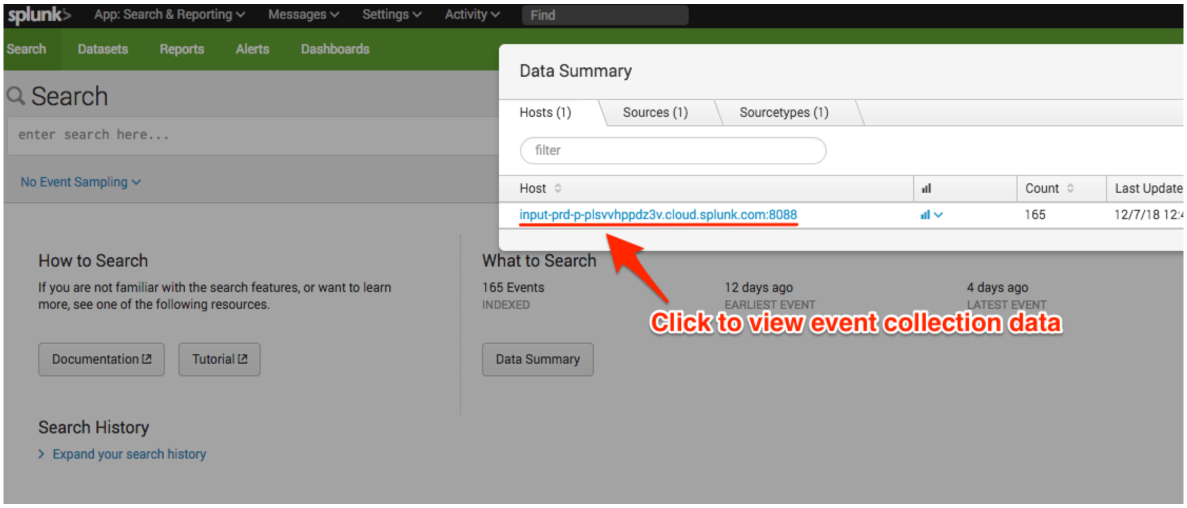
Procedure

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**.

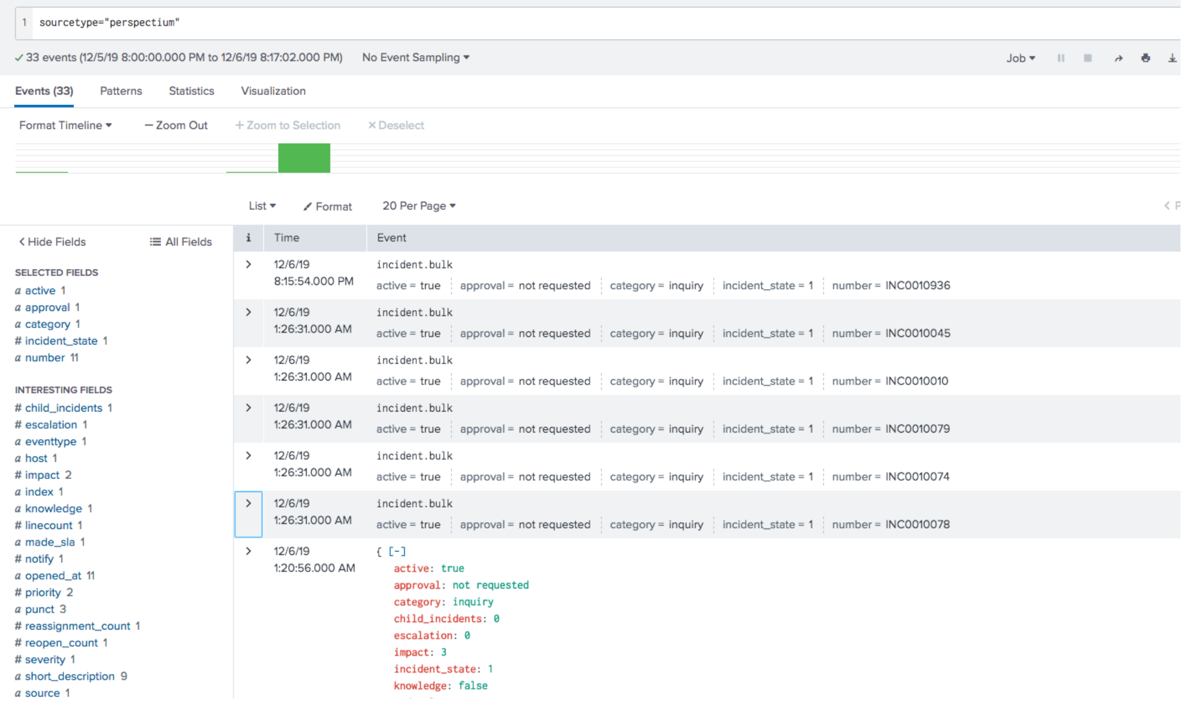
3. On the resulting page, click the **Data Summary** button under **What to Search**. Then, click your Spunk instance name under **Host**.



Host		Count	Last Update
input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088		165	12/7/18 12:

Click to view event collection data

4. Your event collection data will appear on the resulting page.



```
1  sourcetype="perspectium"
```

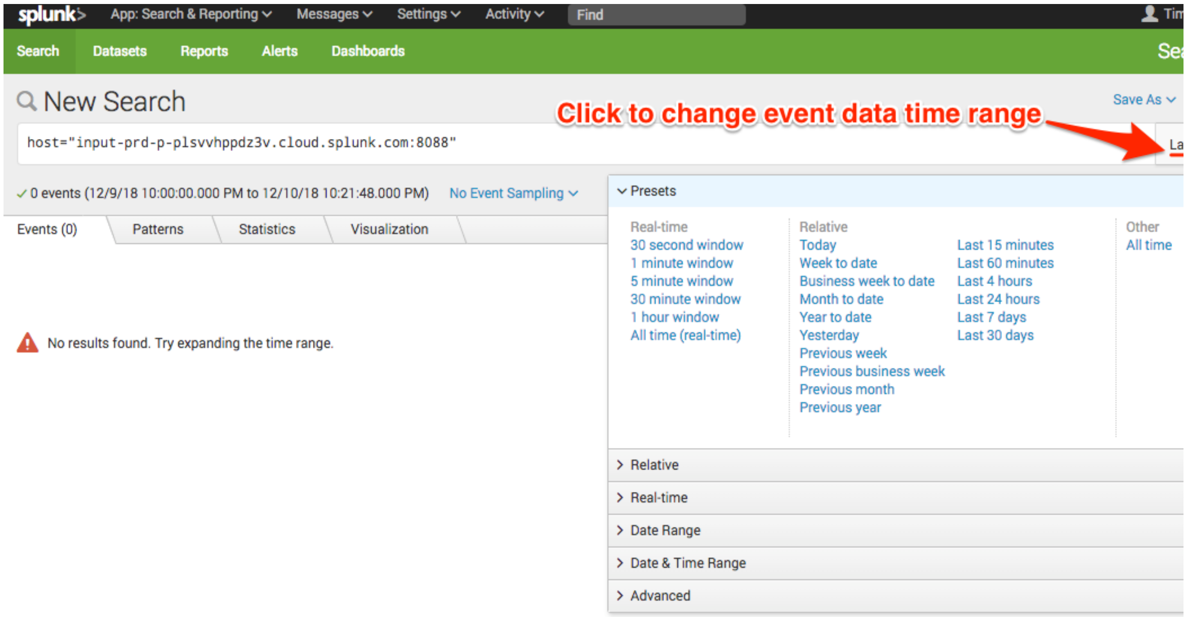
✓ 33 events (12/5/19 8:00:00.000 PM to 12/6/19 8:17:02.000 PM)   No Event Sampling ▾

SELECTED FIELDS
a active 1
a approval 1
a category 1
# incident_state 1
a number 11

INTERESTING FIELDS
# child_incidents 1
# 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.



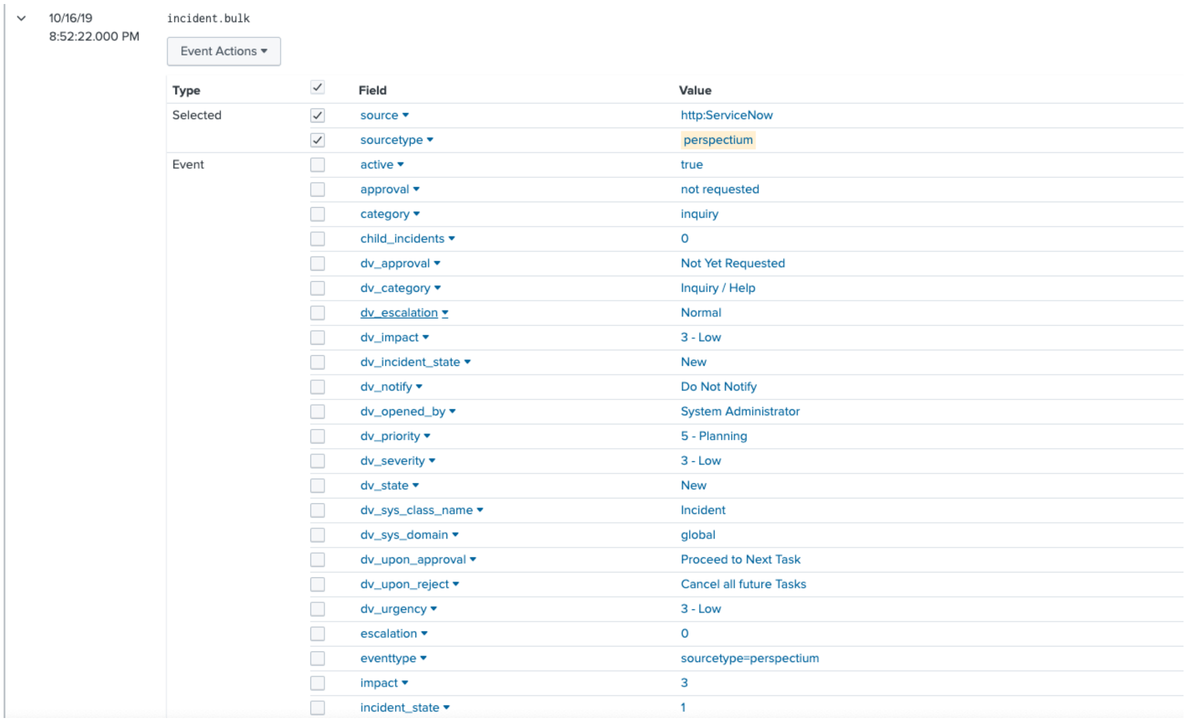
Click to change event data time range

```
host="input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088"
```

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

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:

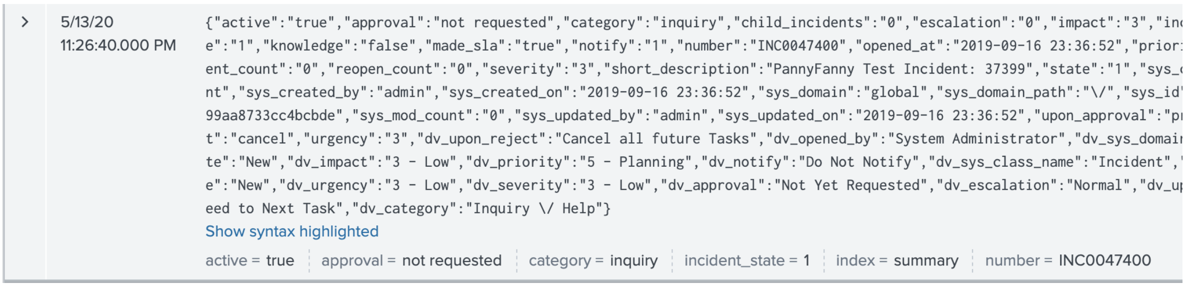


10/16/19
8:52:22.000 PM

incident.bulk

Type	☑	Field	Value
Selected	☑	source ▾	http:ServiceNow
	☑	sourcetype ▾	perspectium
Event	□	active ▾	true
	□	approval ▾	not requested
	□	category ▾	inquiry
	□	child_incidents ▾	0
	□	dv_approval ▾	Not Yet Requested
	□	dv_category ▾	Inquiry / Help
	□	dv_escalation ▾	Normal
	□	dv_impact ▾	3 - Low
	□	dv_incident_state ▾	New
	□	dv_notify ▾	Do Not Notify
	□	dv_opened_by ▾	System Administrator
	□	dv_priority ▾	5 - Planning
	□	dv_severity ▾	3 - Low
	□	dv_state ▾	New
	□	dv_sys_class_name ▾	Incident
	□	dv_sys_domain ▾	global
	□	dv_upon_approval ▾	Proceed to Next Task
	□	dv_upon_reject ▾	Cancel all future Tasks
	□	dv_urgency ▾	3 - Low
	□	escalation ▾	0
	□	eventtype ▾	sourcetype=perspectium
	□	impact ▾	3
	□	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","in
e":"1","knowledge":"false","made_sla":"true","notify":"1","number":"INC0047400","opened_at":"2019-09-16 23:36:52","prior
ent_count":"0","reopen_count":"0","severity":"3","short_description":"PannyFanny Test Incident: 37399","state":"1","sys_
nt","sys_created_by":"admin","sys_created_on":"2019-09-16 23:36:52","sys_domain":"global","sys_domain_path":"\/","sys_id'
99aa8733cc4bcbde","sys_mod_count":"0","sys_updated_by":"admin","sys_updated_on":"2019-09-16 23:36:52","upon_approval":"p
t":"cancel","urgency":"3","dv_upon_reject":"Cancel all future Tasks","dv_opened_by":"System Administrator","dv_sys_domai
te":"New","dv_impact":"3 - Low","dv_priority":"5 - Planning","dv_notify":"Do Not Notify","dv_sys_class_name":"Incident",'
e":"New","dv_urgency":"3 - Low","dv_severity":"3 - Low","dv_approval":"Not Yet Requested","dv_escalation":"Normal","dv_u
eed to Next Task","dv_category":"Inquiry \/ Help"}
```

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.

Similar topics

- Generate a Splunk Event Collector token
- Open Splunk HTTP Event Collector port to the Perspectium Integration Mesh
- DataSync for Splunk
- Get started with DataSync for Splunk
- View your event collections in Splunk

Contact Perspectium Support

☎

US: 1 888 620 8880

UK: 44 208 068 5953

support@perspectium.com