View your event collections in Splunk

Fluorine+

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

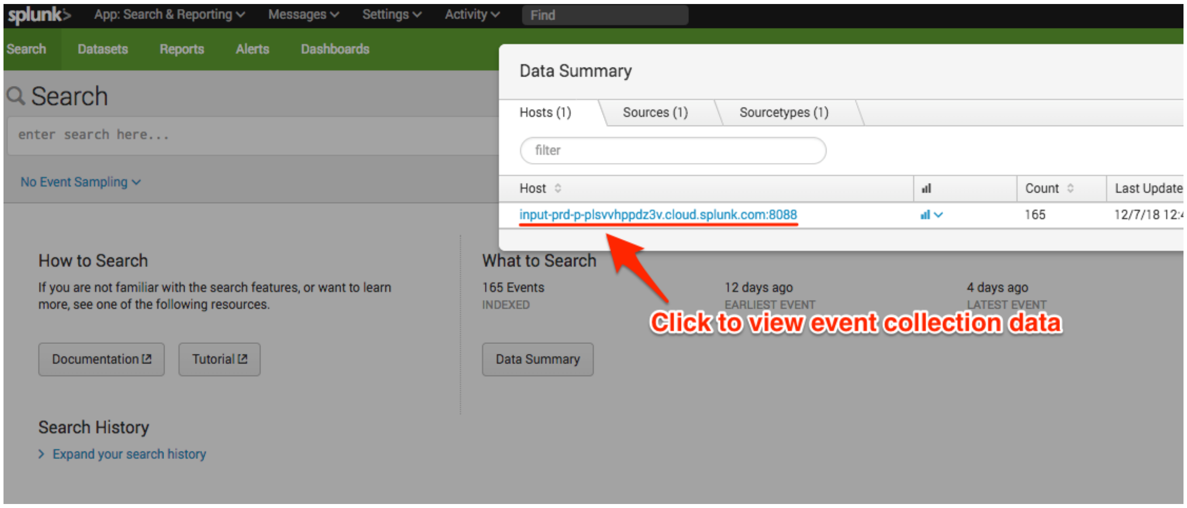
After executing your bulk share for Splunk or creating your dynamic share for Splunk and creating/updating/deleting records, log into your Splunk instance and click the Splunk logo to navigate to your instance's homepage.

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**.

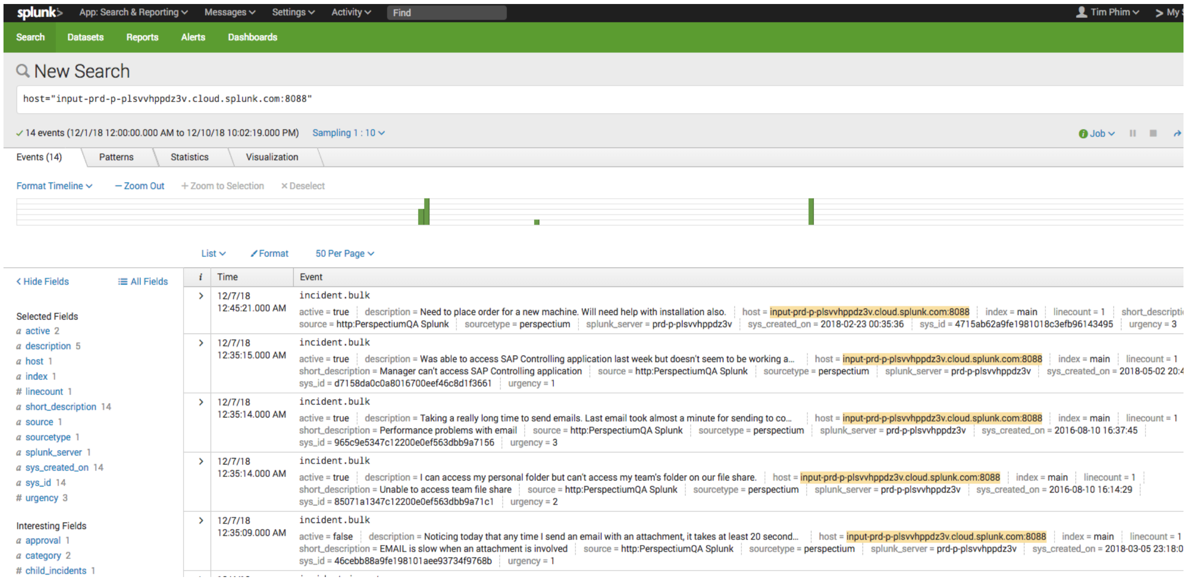


Host		Count	Last Update
input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088		165	12/7/18 12:4

Click to view event collection data

4

Your event collection data will appear on the resulting page.



New Search

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

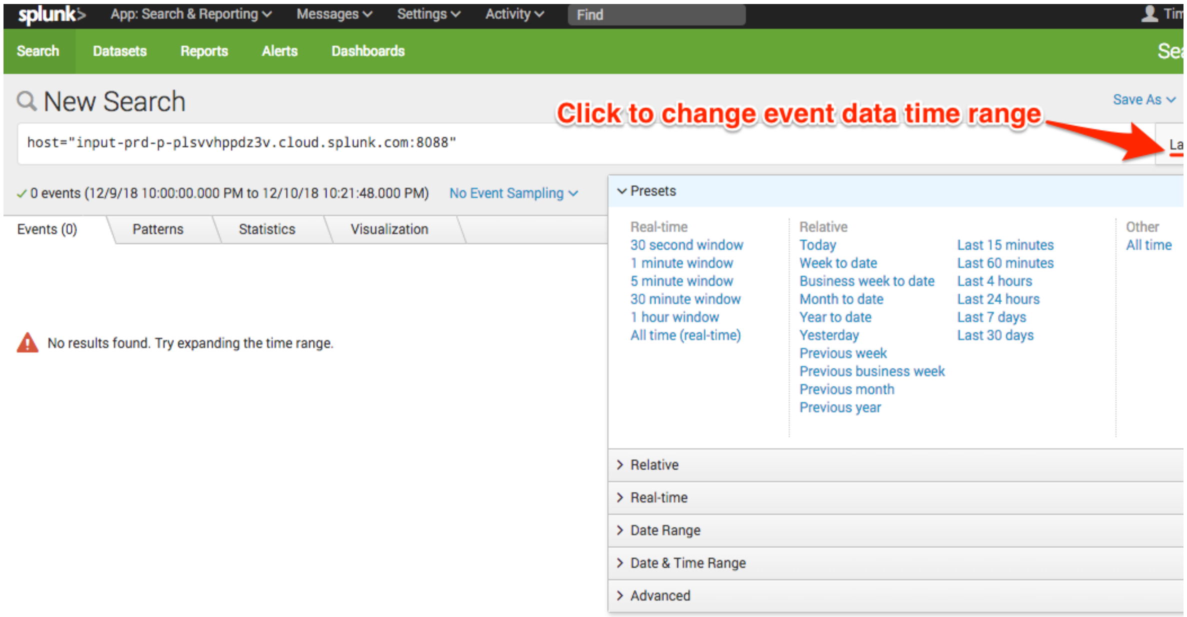
✓ 14 events (12/1/18 12:00:00.000 AM to 12/10/18 10:02:19.000 PM) Sampling 1 : 10

Selected Fields
- a active 2
- a description 5
- a host 1
- a index 1
- # linecount 1
- a short_description 14
- a source 1
- a sourcetype 1
- a splunk_server 1
- a sys_created_on 14
- a sys_id 14
- # urgency 3

Interesting Fields
- a approval 1
- a category 2
- # child_incidents 1

```
i  Time                  Event
>  12/7/18               incident.bulk
   12:45:21.000 AM       active = true | description = Need to place order for a new machine. Will need help with installation also. | host = input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088 | index = main | linecount = 1 | short_descripti
                         source = http:PerspectiumQA Splunk | sourcetype = perspectium | splunk_server = prd-p-plsvvhppdz3v | sys_created_on = 2018-02-23 00:35:36 | sys_id = 4715ab62a9fe1981018c3efb96143495 | urgency = 3
>  12/7/18               incident.bulk
   12:35:15.000 AM       active = true | description = Was able to access SAP Controlling application last week but doesn't seem to be working a... | host = input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088 | index = main | linecount = 1
                         short_description = Manager can't access SAP Controlling application | source = http:PerspectiumQA Splunk | sourcetype = perspectium | splunk_server = prd-p-plsvvhppdz3v | sys_created_on = 2018-05-02 20:4
                         sys_id = d7158da0c0a8016700eef46c8d1f3661 | urgency = 1
>  12/7/18               incident.bulk
   12:35:14.000 AM       active = true | description = Taking a really long time to send emails. Last email took almost a minute for sending to co... | host = input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088 | index = main | linecount = 1
                         short_description = Performance problems with email | source = http:PerspectiumQA Splunk | sourcetype = perspectium | splunk_server = prd-p-plsvvhppdz3v | sys_created_on = 2016-08-10 16:37:45 |
                         sys_id = 965c9e5347c12200e0ef563dbb9a7156 | urgency = 3
>  12/7/18               incident.bulk
   12:35:14.000 AM       active = true | description = I can access my personal folder but can't access my team's folder on our file share. | host = input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088 | index = main | linecount = 1 |
                         short_description = Unable to access team file share | source = http:PerspectiumQA Splunk | sourcetype = perspectium | splunk_server = prd-p-plsvvhppdz3v | sys_created_on = 2016-08-10 16:14:29 |
                         sys_id = 85071a1347c12200e0ef563dbb9a71c1 | urgency = 2
>  12/7/18               incident.bulk
   12:35:09.000 AM       active = false | description = Noticing today that any time I send an email with an attachment, it takes at least 20 second... | host = input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088 | index = main | linecount = 1
                         short_description = EMAIL is slow when an attachment is involved | source = http:PerspectiumQA Splunk | sourcetype = perspectium | splunk_server = prd-p-plsvvhppdz3v | sys_created_on = 2018-03-05 23:18:0
                         sys_id = 46cebb88a9fe198101aee93734f9768b | urgency = 1
```

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.



New Search

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 results found. Try expanding the time range.

Similar topics

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

Contact Perspectium Support

US: 1 888 620 8880

UK: 44 208 068 5953

support@perspectium.com