

View your event collections in Splunk

Fluorine+

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 titled 'Search' and includes a search bar, 'No Event Sampling' dropdown, 'How to Search' section with links to Documentation and Tutorial, and a Search History section. On the right, the 'Data Summary' panel is open, showing a table with columns: Host, Count, and Last Update. The table has one row with the host 'input-prd-p-plsvvhppdz3v.cloud.splunk.com:8088', a count of 165, and a last update of 12/7/18 12:4. Below the table, the 'What to Search' section shows '165 Events INDEXED' and buttons for 'Data Summary' and 'Click to view event collection data' (highlighted with a red arrow).

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

4

Your event collection data will appear on the resulting page.

Splunk Search Results

Search: `host="input-prd-p-plsvhpdz3v.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

Events (14) | Patterns | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect

List | Format | 50 Per Page

< Hide Fields	All Fields	Time	Event
Selected Fields # active 2 # description 5 # host 1 # index 1 # linecount 1 # short_description 14 # source 1 # sourcetype 1 # splunk_server 1 # sys_created_on 14 # sys_id 14 # urgency 3		12/7/18 12:45:21.000 AM	incident.bulk active = true description = Need to place order for a new machine. Will need help with installation also. host = input-prd-p-plsvhpdz3v.cloud.splunk.com:8088 index = main linecount = 1 short_description = Performance problems with email source = http:PerspectiumQA Splunk sourcetype = perspectium splunk_server = prd-p-plsvhpdz3v sys_created_on = 2018-02-23 00:35:36 sys_id = 4715ab62a9fe1981018c3efb96143495 urgency = 3
		12/7/18 12:35:15.000 AM	incident.bulk active = true description = Was able to access SAP Controlling application last week but doesn't seem to be working a... host = input-prd-p-plsvhpdz3v.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-plsvhpdz3v sys_created_on = 2018-05-02 20:47:15ab62a9fe1981018c3efb96143495 urgency = 1
		12/7/18 12:35:14.000 AM	incident.bulk 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-plsvhpdz3v.cloud.splunk.com:8088 index = main linecount = 1 short_description = Performance problems with email source = http:PerspectiumQA Splunk sourcetype = perspectium splunk_server = prd-p-plsvhpdz3v sys_created_on = 2016-08-10 16:37:45 sys_id = 965c9e5347c12200e0ef563dbb9a7156 urgency = 3
		12/7/18 12:35:14.000 AM	incident.bulk 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-plsvhpdz3v.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-plsvhpdz3v sys_created_on = 2016-08-10 16:14:29 sys_id = 85071a1347c12200e0ef563dbb9a71c1 urgency = 2
Interesting Fields # approval 1 # category 2 # child_incidents 1		12/7/18 12:35:09.000 AM	incident.bulk 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-plsvhpdz3v.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-plsvhpdz3v sys_created_on = 2018-03-05 23:18:03 sys_id = 46cebb88a9fe198101aee937349768b 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.

Splunk Search Interface

Search: `host="input-prd-p-plsvhpdz3v.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

Events (0) | Patterns | Statistics | Visualization

⚠ No results found. Try expanding the time range.

Click to change event data time range

Presets

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

Relative
Real-time
Date Range
Date & Time Range
Advanced

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