

Cerinte de lucru in laborator - Splunk

Logare Splunk.

Ingest actions este o nouă interfață cu utilizatorul care permite clienților să configureze rapid și ușor fluxurile de date și să controleze volumul, formatul și destinația datelor. Este accesibil din aplicația Splunk Enterprise și Splunk Cloud Platform Search and Reporting ca opțiune în meniul derulant administrativ.

Utilizați acțiuni de asimilare pentru a filtra, masca și direcționa datele la asimilare și la margine, folosind doar clicuri simple - fără scrierea liniilor de comandă sau strofe de mână în fișierele de configurare. Această caracteristică vă permite să eliminați zgomotul, descurcând datele esențiale de cele care trebuie arhivate.

KNOWLEDGE	DATA
Searches, reports, and alerts	Data inputs
Data models	Forwarding and receiving
Event types	Indexes
Tags	Report acceleration summaries
Fields	Virtual indexes
Lookups	Source types
User interface	Ingest actions
Alert actions	

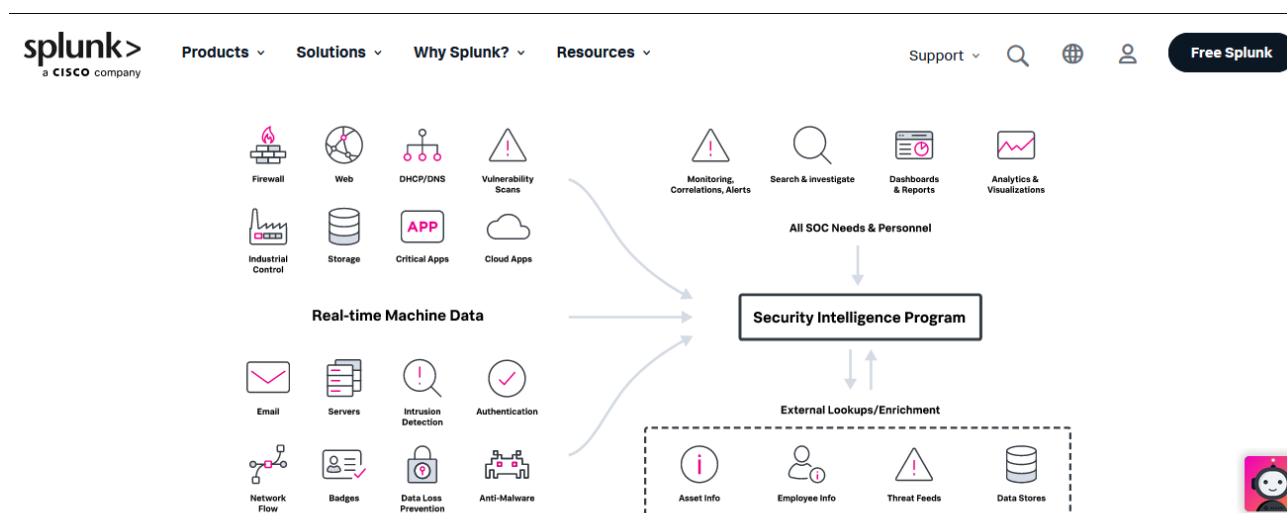
1. Analizați linkul și explicați rolul lui **Ingest actions**.

https://lantern.splunk.com/Splunk_Platform/Getting_Started/Getting_data_into_Cloud_Platform?mt-learningpath=cloudstart&_gl=1*1wkylnm*_ga*MTUyODk5MTA5Mi4xNzEyNzc1NjU2*_ga_5EPM2P39FV*MTcxMjc3NTY1NS4xLjEuMTcxMjc3NTY4Mi4wLjAuMTY2OTAxMDU1OQ..*_ga_GS7YF8S63Y*MTcxMjc3NTY2Mi4xLjEuMTcxMjc3NTY3OC40NC4wLjA.&_ga=2.51345580.401423552.1712775657-1528991092.1712775656&_gac=1.226176616.1712775677.CjwKCAjw8diwBhAbEiwA7i_sJaSl4D6RDpMfbp1zHPpUM6XOc3K4E3zHGylDxNvPquEd_MZ54AJyshoCziUQAvD_BwE

2. Cu Splunk puteți să:

- Colectați și indexați toate datele mașinii dvs. pentru a permite cunoașterea situației de la capăt la capăt
- Obțineți o mai bună vizibilitate asupra operațiunilor IT și a cerințelor de date pentru reglementări și mandate
- Monitorizați rețelele din învățământul superior pentru a asigura securitatea, conformitatea și reducerea riscurilor rentabile
- Sprijină raportarea ad-hoc și monitorizarea în timp real a incidentelor și atacurilor, astfel încât echipele de securitate să poată fi mai proactive în răspunsul la amenințări
- Reduceți costurile pentru operațiuni mai eficiente și decizii mai bune la nivelul instituției de învățământ în ansamblu.

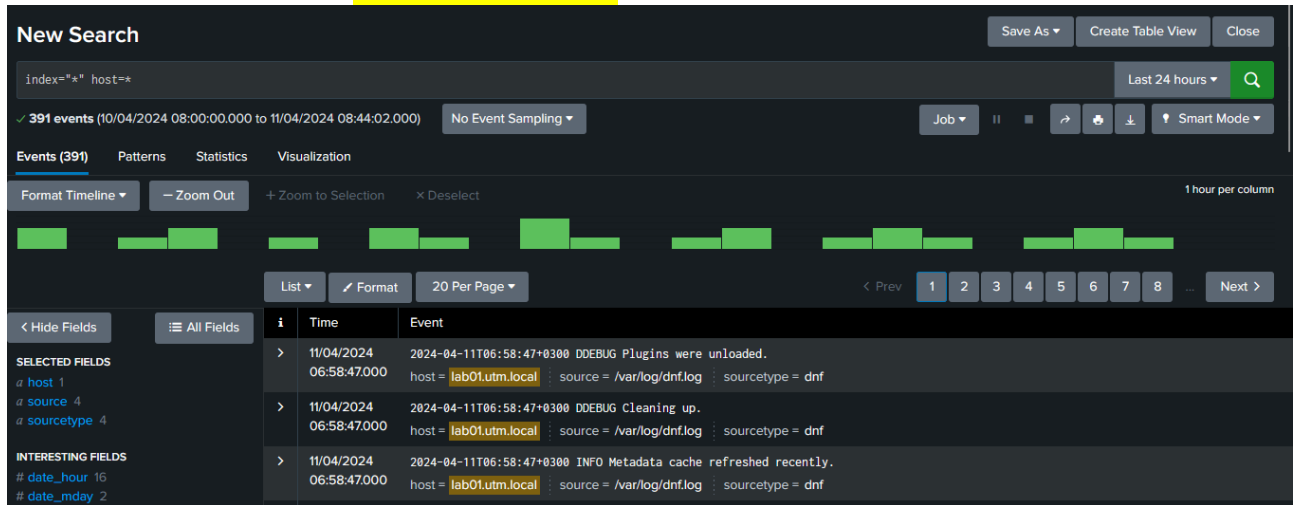
Platforma Splunk poate citi date din aproape orice sursă imaginabilă, inclusiv sisteme de înregistrare a studenților, sisteme de management al învățării, rețele, servere web, fișiere jurnal, date firewall, senzori la distanță, aplicații mobile și online de învățare, aplicații vechi, servere de aplicații și baze de date structurate. Platforma Splunk utilizează date neexploatate ale mașinii pentru a identifica problemele, riscurile și oportunitățile pentru a reduce costuri și pentru a oferi operațiuni mai eficiente, precum și pentru a face instituțiile de învățământ mai sigure.



Analizați linkul și scrieți 2 idei principale cu privire la rolul acestuia

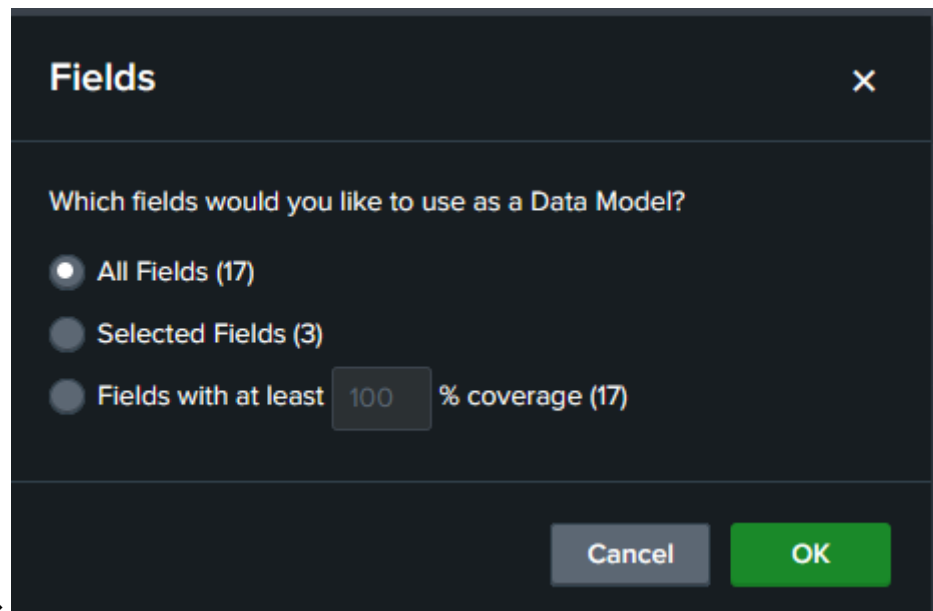
https://www.splunk.com/en_us/solutions/industries/higher-education.html?_gl=1*1rgwii3*_ga*MTUyODk5MTA5Mi4xNzEyNzc1NjU2*_ga_GS7YF8S63Y*MTcxMjc3NTY2Mi4xLjEuMTcxMjc3NTg1MS4xMC4wLjA.*_ga_5EPM2P39FV*MTcxMjc3NTY1NS4xLjEuMTcxMjc3NTg1Mi4wLjAuMTY2OTAxMDU1OQ..&_ga=2.254308365.401423552.1712775657-1528991092.1712775656&_gac=1.190008025.1712775677.CjwKCAjw8diwBhAbEiwA7i_sJaSl4D6RDpMfbp1zHPpUM6XOc3K4E3zHGylDxNvPquEd_MZ54AJyshoCziUQAvD_BwE

3. Sa se realizeze cautare `index="*" host=*`



The screenshot shows the Splunk Search interface. At the top, the search bar contains the query `index="*" host=*`. Below the search bar, the results are displayed in a table view. The table has columns for Time and Event. The first three rows of data are visible, showing events from 11/04/2024 06:58:47.000. The events are related to DDEBUG Plugins and DDEBUG Cleaning up. The interface also includes a visualization section with a timeline view and a list of fields on the left.

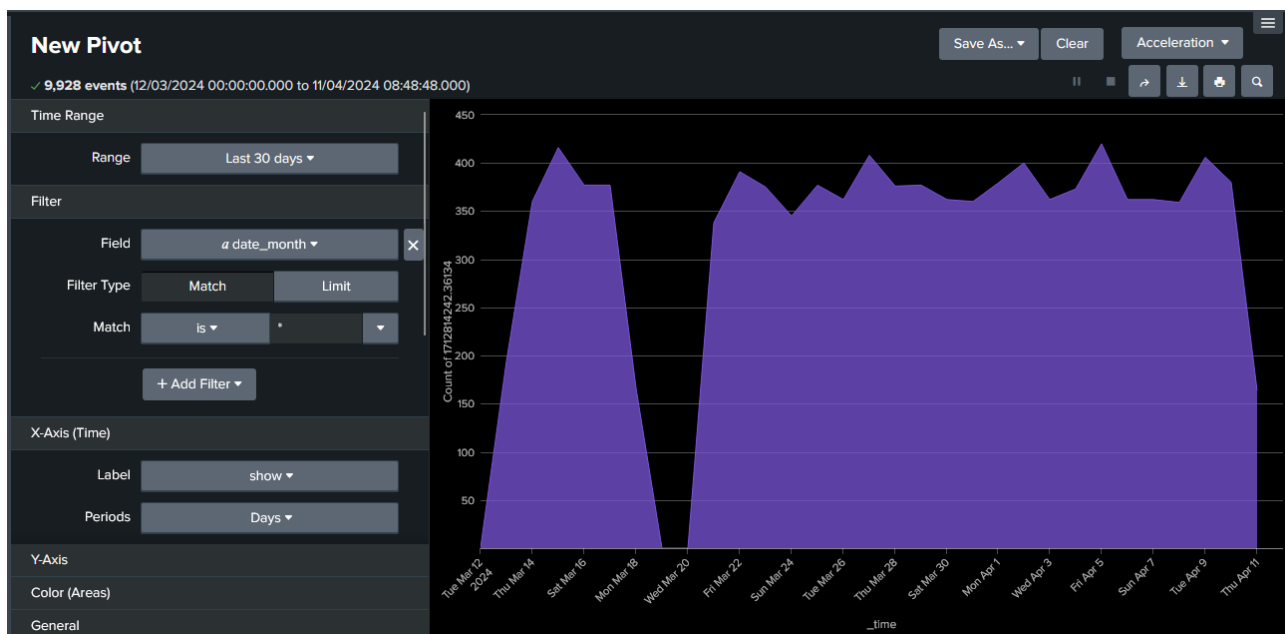
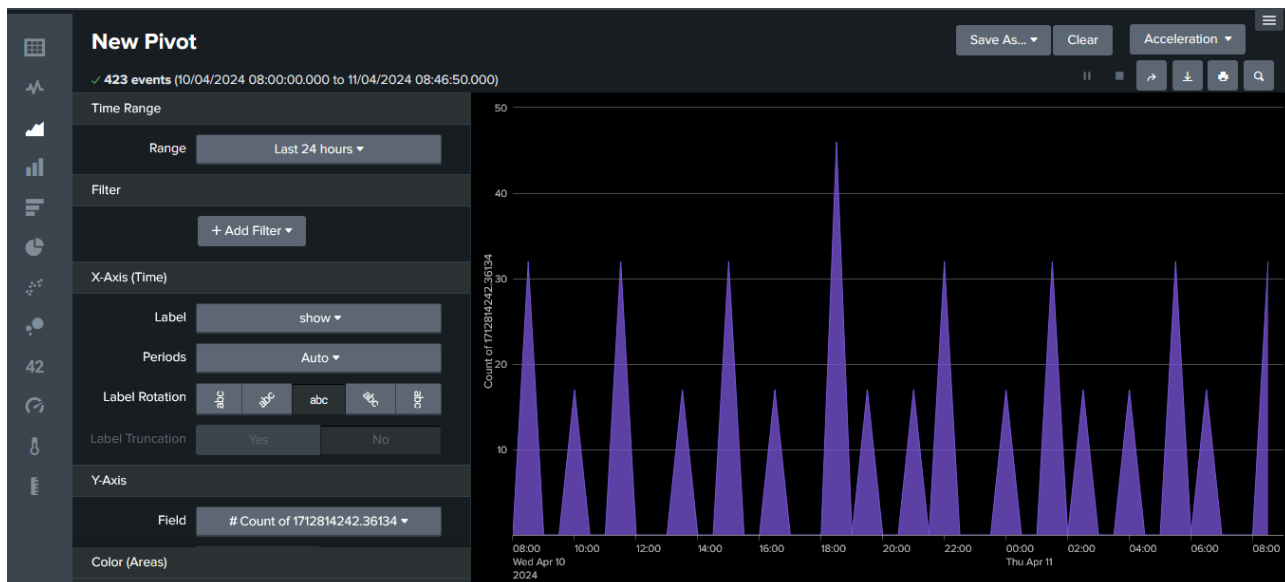
i	Time	Event
>	11/04/2024 06:58:47.000	2024-04-11T06:58:47+0300 DDEBUG Plugins were unloaded. host = lab01.utm.local : source = /var/log/dnf.log : sourcetype = dnf
>	11/04/2024 06:58:47.000	2024-04-11T06:58:47+0300 DDEBUG Cleaning up. host = lab01.utm.local : source = /var/log/dnf.log : sourcetype = dnf
>	11/04/2024 06:58:47.000	2024-04-11T06:58:47+0300 INFO Metadata cache refreshed recently. host = lab01.utm.local : source = /var/log/dnf.log : sourcetype = dnf



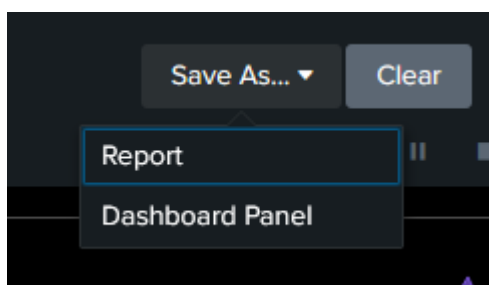
The screenshot shows the 'Fields' dialog box in Splunk. The dialog asks 'Which fields would you like to use as a Data Model?'. There are three radio button options: 'All Fields (17)', 'Selected Fields (3)', and 'Fields with at least 100 % coverage (17)'. The 'All Fields (17)' option is selected. At the bottom, there are 'Cancel' and 'OK' buttons.

→ Visualization→Pivot→

Si apoi sa se obtina diverse tipuri de grafice, ca de exemplu:



Sa se salveze pe Dashboard cu numele Studentului.



Save As Dashboard Panel

Dashboard ID ?

10

The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.

Dashboard Description

optional

Dashboard Permissions

Private

Shared in App

Panel Title

optional

Panel Powered By ?

Q Inline Search

Drilldown ?

No action

Panel Content

Statistics

Area Chart

You must save the original search as a data model. This will power the Dashboard Panel.

Model Title

Grafic_1

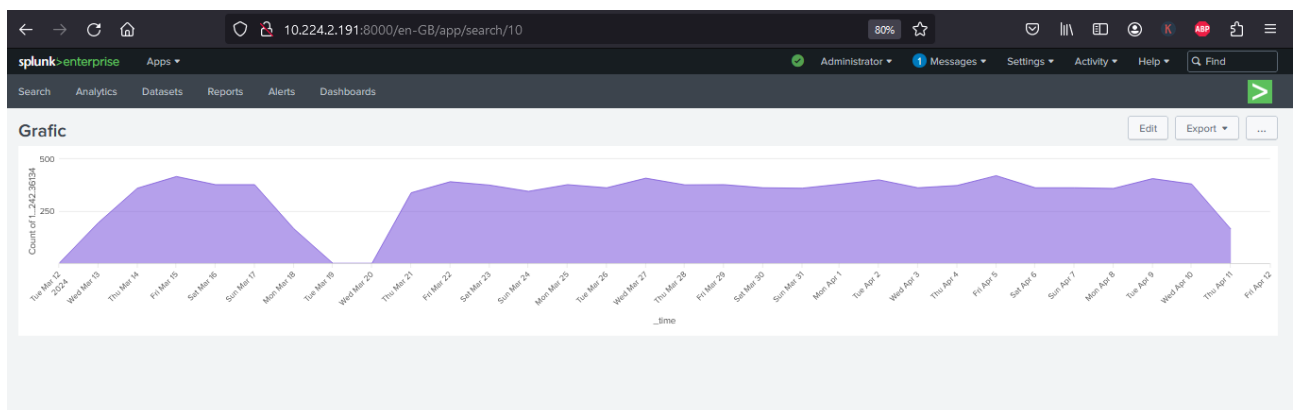
Model ID ?

Grafic_1

The data model ID can only contain letters, numbers, dashes, and underscores. Do not start the data model ID with a period.

Cancel

Save



Sa se analizeze codul sursa al graficului

 No validation issues

```

1 <dashboard version="1.1">
2 <label>Grafic</label>
3 <row>
4 <panel>
5 <chart>
6 <search>
7 <query>| pivot Grafic_1 RootObject count(RootObject) AS "Count of 1712814242.36134" SPLITROW _time AS _time PERIOD day FILTER date_month is "*" SORT 0 _time ROWSUMMARY 0
8 SHOWOTHER 1</query>
9 <earliest>30d</earliest>
10 <latest>now</latest>
11 <sampleRatio>1</sampleRatio>
12 </search>
13 <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>
14 <option name="charting.axisLabelsX.majorLabelStyle.rotation">-45</option>
15 <option name="charting.axisTitleX.visibility">visible</option>
16 <option name="charting.axisTitleY.visibility">visible</option>
17 <option name="charting.axisTitleY2.visibility">visible</option>
18 <option name="charting.axisX.abbreviation">none</option>
19 <option name="charting.axisX.scale">linear</option>
20 <option name="charting.axisY.abbreviation">none</option>
21 <option name="charting.axisY.scale">linear</option>
22 <option name="charting.axisY2.abbreviation">none</option>
23 <option name="charting.axisY2.enabled">0</option>
24 <option name="charting.axisY2.scale">inherit</option>
25 <option name="charting.chart">area</option>
26 <option name="charting.chart.bubbleMaximumSize">50</option>
27 <option name="charting.chart.bubbleMinimumSize">10</option>
28 <option name="charting.chart.bubbleSizeBy">area</option>
29 <option name="charting.chart.nullValueMode">gaps</option>
30 <option name="charting.chart.showDataLabels">none</option>
31 <option name="charting.chart.sliceCollapsingThreshold">0.01</option>
32 <option name="charting.chart.stackMode">default</option>
33 <option name="charting.chart.style">shiny</option>

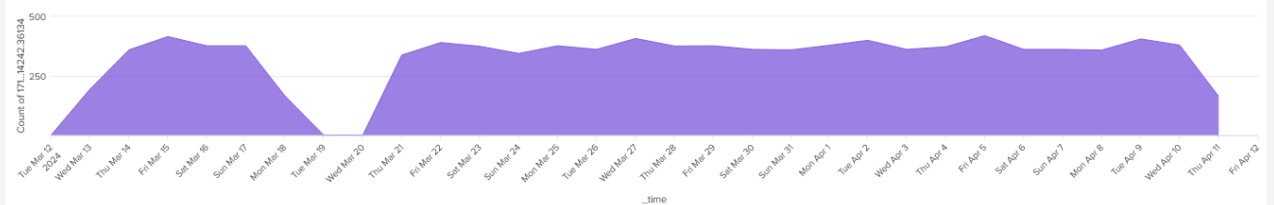
```

Grafic Copy

No description

No title

No title



Sa se analizeze codul:

```
<dashboard>
  <label>Masterand_UTM</label>
  <row>
    <panel>
      <event>
        <search>
          <query>index="main"</query>
          <earliest>-30d@d</earliest>
          <latest>now</latest>
          <sampleRatio>1</sampleRatio>
        </search>
        <option name="list.drilldown">full</option>
        <option name="list.wrap">1</option>
        <option name="maxLines">5</option>
        <option name="raw.drilldown">full</option>
        <option name="rowNumbers">0</option>
        <option name="table.drilldown">none</option>
        <option name="table.sortDirection">asc</option>
        <option name="table.wrap">1</option>
        <option name="type">table</option>
      </event>
    </panel>
  </row>
</dashboard>
```

Modificati acest cod, pentru a extrage evenimentele din ultimele 60 minute din oricare index.

No validation issues

```
<dashboard>
  <label>Masterand_UTM</label>
  <row>
    <panel>
      <event>
        <search>
          <query>index="main"</query>
          <earliest>-15m@m</earliest>
          <latest>now</latest>
          <sampleRatio>1</sampleRatio>
        </search>
        <option name="list.drilldown">full</option>
        <option name="list.wrap">1</option>
        <option name="maxLines">5</option>
        <option name="raw.drilldown">full</option>
        <option name="rowNumbers">0</option>
        <option name="table.drilldown">none</option>
        <option name="table.sortDirection">asc</option>
        <option name="table.wrap">1</option>
        <option name="type">table</option>
      </event>
    </panel>
  </row>
</dashboard>
```

4. **Aplicația Splunk Machine Learning Toolkit** oferă noi comenzi SPL, vizualizări personalizate, asistenți și exemple pentru a explora o varietate de concepte pentru ML.

Fiecare asistent include exemple cu seturi de date, plus capacitatea de a aplica vizualizările și comenzile SPL la propriile date. Puteți inspecta panourile de asistență și codul de bază pentru a vedea cum funcționează totul.

Căutați lista noastră de redare ML Youtube pentru explicații simple despre cum să utilizați MLTK și pentru ce este acesta.

<https://docs.splunk.com/images/3/3f/Splunk-MLTK-QuickRefGuide-2019-web.pdf>

Rolul aplicației **Splunk Machine Learning Toolkit** →

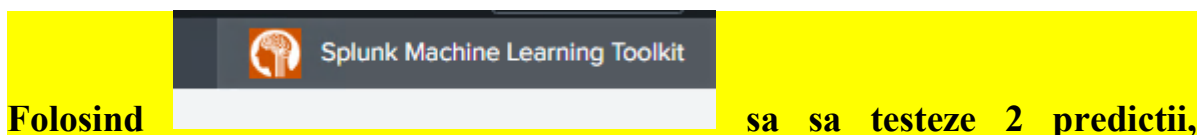
<https://splunkbase.splunk.com/app/2890>

Sa sa lucreze tutorialele →

<https://www.youtube.com/watch?v=GGw8tpzh4Ns>

<https://www.youtube.com/watch?v=mWhwR3DNmxU>

5. <https://docs.splunk.com/Documentation/MLEApp/5.4.1/User/WelcomeToMLTK>



exemplu → Predict Disk Utilization care utilizează Asistentul de predicție inteligentă și algoritmul de predicție automată pentru a prezice utilizarea discului din câmpurile din date, inclusiv accesul la disc și blocurile de disc, sa se realizeze predictia utilizarii discului in ultimele 24 de ore.

←→↺🏠

🔒 10.224.2.191:8000/en-GB/app/Splunk_ML_Toolkit/contents

90%★

🔔📄👤🔑📁🔍

splunk-enterprise Apps

🚨 Administrator 1 Messages Settings Activity Help Find

Showcase Experiments Search Models Settings Docs Video Tutorials

Splunk Machine Learning Toolkit

Showcase


Welcome to the Machine Learning Toolkit Showcase. Watch and learn from interactive end-to-end examples using real datasets. Click on an example to pre-populate the Assistant with the sample dataset and its settings. Inspect the Search Processing Language as well as the underlying code of these examples to see how it all works.

View examples by

ML Operation Industry

Filter Examples 🔍


Predict Fields



View examples that predict the value of a numeric or categorical field using the values from other fields in the event.

15 Examples Available


Detect Outliers



View examples that detect numeric and categorical values that differ significantly from values in the rest of the data. Identified outliers are indicative of interesting, unusual, and possibly dangerous events.

14 Examples Available


Forecast Time Series



View examples that predict the next value in a sequence of time series data by using past time series data.

9 Examples Available

Cluster Events



View examples that partition events with multiple fields into groups of events based on the values of those fields.

▼ Featured Examples

Predict Disk Utilization

This example uses the Smart Prediction Assistant and the AutoPrediction algorithm to predict disk utilization from fields in the data including disk access and disk blocks.

IT

Predict Hard Drive Failure

This example uses the Predict Categorical Fields Assistant and the Logistic Regression algorithm to predict disk failure from fields including hard drive model.

IT

Predict Server Power Consumption

This example uses the Predict Numeric Fields Assistant and the Linear Regression algorithm to predict AC power consumption from fields including CPU utilization, disk utilization, and unhalted core cycles.

IT

Predict the Presence of Malware

This example uses the Predict Categorical Fields Assistant and the Logistic Regression algorithm to predict malware from fields including bytes received, bytes sent, and destination port.

Security

Predict the Presence of Vulnerabilities

This example uses the Smart Prediction Assistant and the AutoPrediction algorithm to predict vulnerabilities in firewall data from fields in the data including bytes received, bytes sent, packets received, and packets sent.

Security

Predict VPN Usage

This example uses the Predict Numeric Fields Assistant and the Linear Regression algorithm to predict remote access to the VPN from four other fields.

Security

Smart Prediction

Predict Numeric Fields

Predict Categorical Fields

Smart Prediction Examples

Predict the value of a categorical or numeric field based on one or more other fields in the event using a step-by-step guided workflow.

Predict Disk Utilization

This example uses the Smart Prediction Assistant and the AutoPrediction algorithm to predict disk utilization from fields in the data including disk access and disk blocks.

Predict the Presence of Vulnerabilities

This example uses the Smart Prediction Assistant and the AutoPrediction algorithm to predict vulnerabilities in firewall data from fields in the data including bytes received, bytes sent, packets received, and packets sent.

Smart Prediction: Predict Disk Utilization

CancelNext>

Define

Learn

Review

Define Data Source

SearchDatasetsMetrics

inputlookup server_power.csv

All time

🔍

✓ 31,272 results (01/01/1970 02:00:00.000 to 11/04/2024 11:42:21.000)

Job

Smart Mode

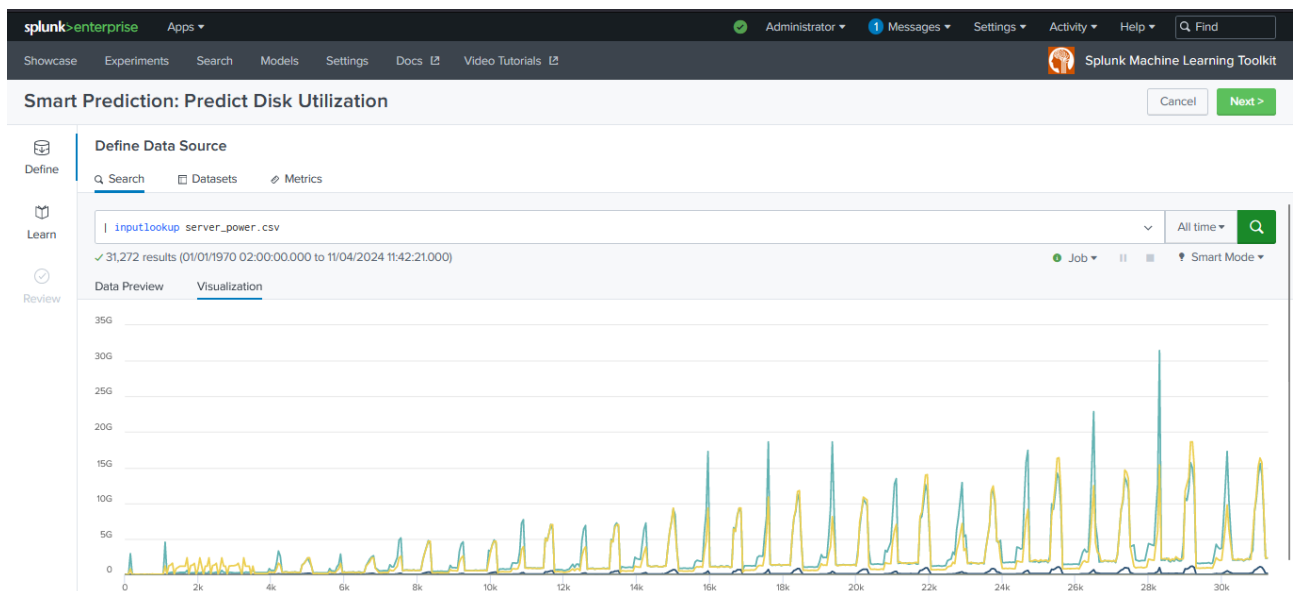
Data Preview

Visualization

20 Per Page

« Prev12345678910Next»

_time	ac_power	total-cpu-utilization	total-disk-accesses	total-disk-blocks	total-disk-utilization	total-instructions_retired	total-last_level_cache_references	total-memory_bus
13:51:28 2008-Apr-14	220.0	0.99	0	0	0	3924639	75140	
13:51:29 2008-Apr-14	220.0	1.15	5.49	214.63	3.66	28433358	59082	
13:51:30 2008-Apr-14	223.0	0.99	30.43	817.39	30.43	10417228	360018	
13:51:31 2008-Apr-14	220.0	0.00	0	0	0	3985700	80619	
13:51:32 2008-Apr-14	220.0	0.99	0	0	0	3788243	68477	
13:51:33 2008-Apr-14	220.0	0.00	0	0	0	4004741	79560	
13:51:34 2008-Apr-14	220.0	0.99	0	0	0	3803393	77156	
13:51:35 2008-Apr-14	219.0	0.00	0	0	0	4820481	114525	
13:51:36 2008-Apr-14	221.0	0.00	23.68	357.89	14.74	6715741	128729	



Smart Prediction: Predict Disk Utilization

CancelNext>

Define

Learn

Review

Define Data Source

SearchDatasetsMetrics

inputlookup server_power.csv

All time

🔍

✓ 31,272 results (01/01/1970 02:00:00.000 to 11/04/2024 11:42:21.000)

Job

Smart Mode

Data Preview

Visualization