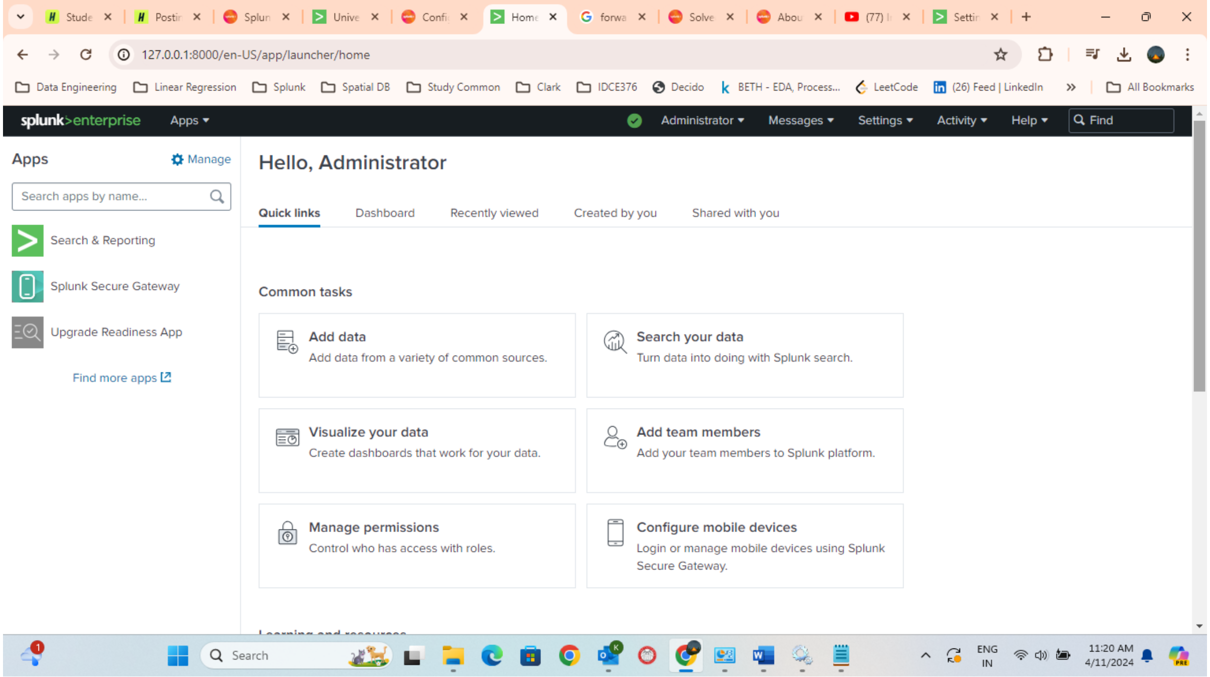
Data Ingestion (Windows real-time performance matrices and Upload method) and Regular Expression Example

1. **Install Splunk on System. Open URL for Splunk enterprise**
   http://127.0.0.1:8000/
2. **Login To Splunk Enterprise**



127.0.0.1:8000/en-US/app/launcher/home

Hello, Administrator

Common tasks

Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your data.

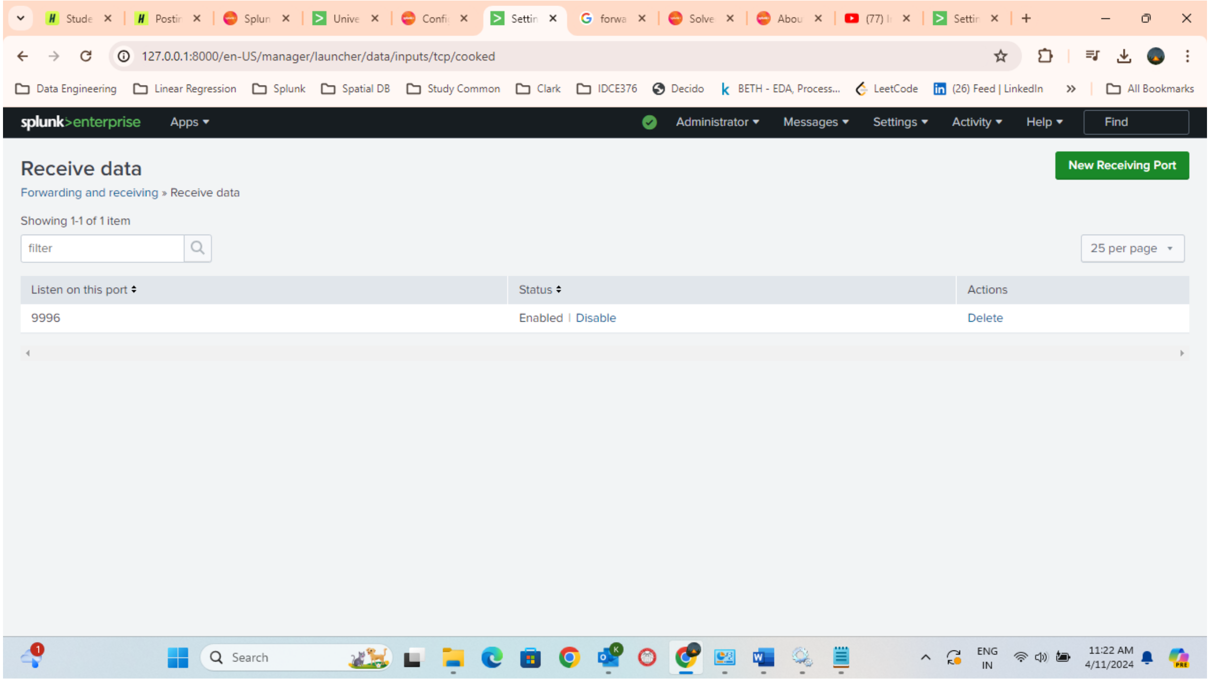
Add team members
Add your team members to Splunk platform.

Manage permissions
Control who has access with roles.

Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

FOR WINDOWS PERFORMANCE MATRICES AND WINDOWS LOGS

3. **Enable Receiver for Splunk Deployment through Settings > Forwarding and receiving > Receive data > Add New**



Receive data

Forwarding and receiving » Receive data

Showing 1-1 of 1 item

Listen on this port	Status	Actions
9996	Enabled | Disable	Delete

4. **Download Splunk Forwarder for Windows OS from** https://www.splunk.com/en_us/download/universal-forwarder.html . Download 64-bit version. Install with standard options.

5. **Edit file input.conf [C:\Program Files\SplunkUniversalForwarder\etc\system\local\]. For performance matices of windows systems (like CPU, Memory, disk), and application & security logs.**

```
[perfmon://Windows__Processor]
counters = % C1 Time;% C2 Time;% Idle Time;% Processor Time;% User Time;% Privileged Time;% Reserved Time;% Interrupt Time
instances = *
interval = 30
object = Processor
sourcetype = PerfmonMetrics:CPU
disabled = 0

## Memory
[perfmon://Windows__Memory]
counters = Cache Bytes;% Committed Bytes In Use;Page Reads/sec;Pages Input/sec;Pages Output/sec;Committed Bytes;Available Bytes
interval = 30
object = Memory
sourcetype = PerfmonMetrics:Memory
disabled = 0

## Physical Disk
```

```
[perfmon://Windows__PhysicalDisk]
counters = % Disk Read Time;% Disk Write Time
instances = *
interval = 30
object = PhysicalDisk
sourcetype = PerfmonMetrics:PhysicalDisk
disabled = 0

## Logical Disk
[perfmon://Windows__LogicalDisk]
counters = Free Megabytes;% Free Space
instances = *
interval = 30
object = LogicalDisk
sourcetype = PerfmonMetrics:LogicalDisk
disabled = 0

## Network
[perfmon://Windows__Network Interface]
counters = Bytes Received/sec;Bytes Sent/sec;Packets Received/sec;Packets Sent/sec;Packets
Received Errors;Packets Outbound Errors
instances = *
interval = 30
object = Network Interface
sourcetype = PerfmonMetrics:Network
disabled = 0

## System
[perfmon://Windows__System]
counters = Processor Queue Length;Threads;System Up Time
instances = *
interval = 30
object = System
sourcetype = PerfmonMetrics:System
disabled = 0

## Process
[perfmon://Windows__Process]
counters = % Processor Time;% User Time;% Privileged Time;Elapsed Time;ID Process;Virtual
Bytes;Working Set;Private Bytes;IO Read Bytes/sec;IO Write Bytes/sec
instances = *
interval = 30
object = Process
sourcetype = PerfmonMetrics:Process
disabled = 0

[monitor://$SPLUNK_HOME\var\log\splunk\*.log*]
sourcetype = uf
```

```
disabled = false
index = _internal

[WinEventLog://Application]
checkpointInterval = 10
current_only = 0
disabled = 0
index = hoth_win_logs
start_from = oldest

[WinEventLog://Security]
checkpointInterval = 10
current_only = 0
disabled = 0
index = hoth_win_logs
start_from = oldest

[WinEventLog://System]
checkpointInterval = 10
current_only = 0
disabled = 0
index = hoth_win_logs
start_from = oldest

[WinEventLog://Setup]
checkpointInterval = 10
current_only = 0
disabled = 0
index = hoth_win_logs
start_from = oldest
```

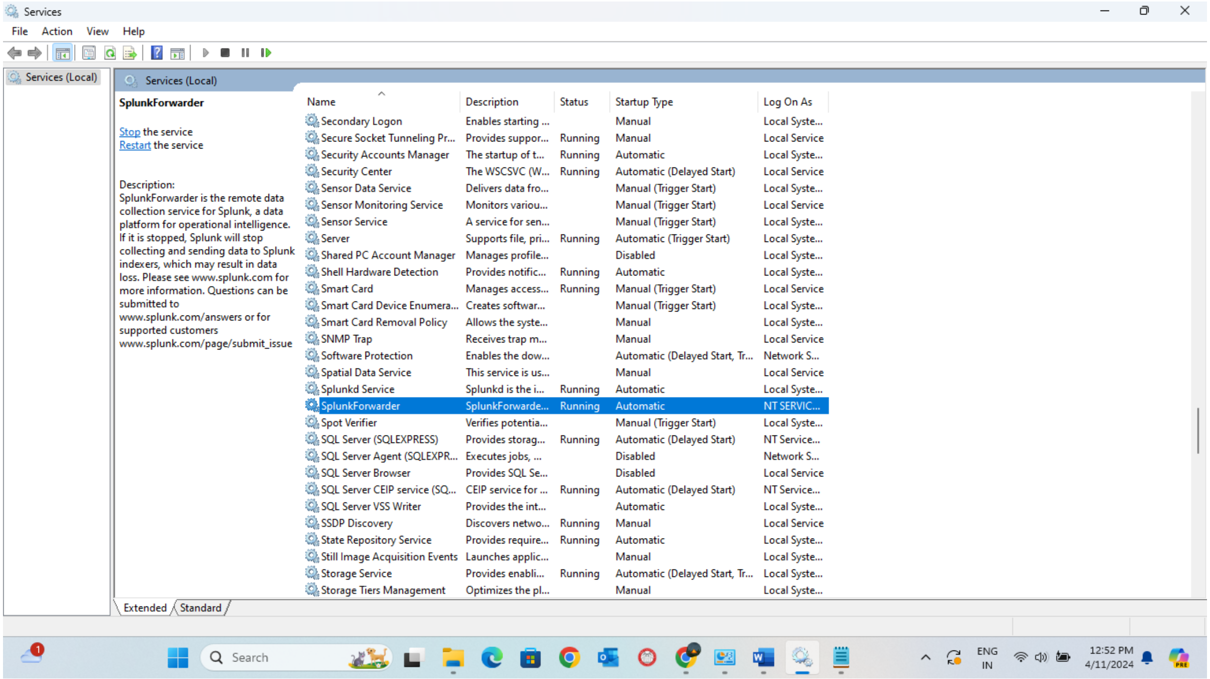
6. **Edit output.conf [C:\Program Files\SplunkUniversalForwarder\etc\system\local\]. For telling destination.**

   ```
   [tcpout]
   defaultGroup = default-autolb-group

   [tcpout:default-autolb-group]
   server = localhost:9996

   [tcpout-server://localhost:9996]
   ```

7. **Restart the service**



SplunkForwarder

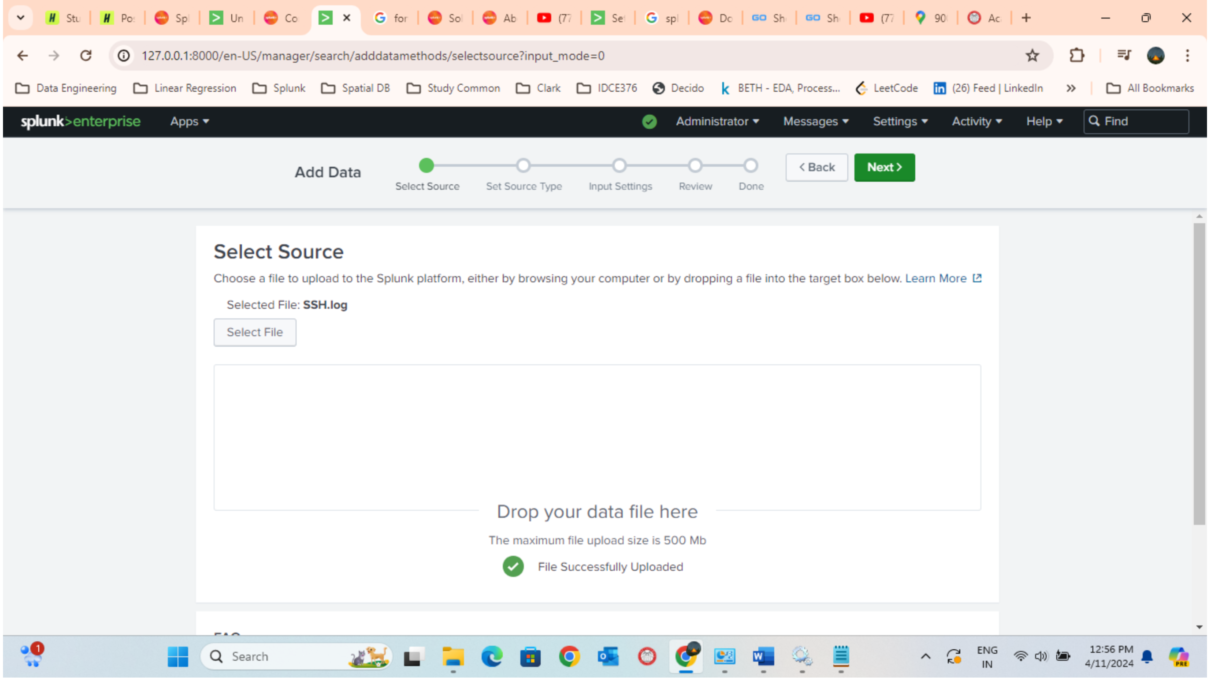
Stop the service
Restart the service

Description:
SplunkForwarder is the remote data collection service for Splunk, a data platform for operational intelligence. If it is stopped, Splunk will stop collecting and sending data to Splunk indexers, which may result in data loss. Please see www.splunk.com for more information. Questions can be submitted to www.splunk.com/answers or for supported customers www.splunk.com/page/submit_issue

Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables starting ...		Manual	Local Syste...
Secure Socket Tunneling Pr...	Provides suppor...	Running	Manual	Local Service
Security Accounts Manager	The startup of t...	Running	Automatic	Local Syste...
Security Center	The WSCSVC (W...	Running	Automatic (Delayed Start)	Local Service
Sensor Data Service	Delivers data fro...		Manual (Trigger Start)	Local Syste...
Sensor Monitoring Service	Monitors variou...		Manual (Trigger Start)	Local Service
Sensor Service	A service for sen...		Manual (Trigger Start)	Local Syste...
Server	Supports file, pri...	Running	Automatic (Trigger Start)	Local Syste...
Shared PC Account Manager	Manages profile...		Disabled	Local Syste...
Shell Hardware Detection	Provides notific...	Running	Automatic	Local Syste...
Smart Card	Manages access...	Running	Manual (Trigger Start)	Local Service
Smart Card Device Enumera...	Creates softwar...		Manual (Trigger Start)	Local Syste...
Smart Card Removal Policy	Allows the syste...		Manual	Local Syste...
SNMP Trap	Receives trap m...		Manual	Local Service
Software Protection	Enables the dow...		Automatic (Delayed Start, Tr...	Network S...
Spatial Data Service	This service is us...		Manual	Local Service
Splunkd Service	Splunkd is the i...	Running	Automatic	Local Syste...
SplunkForwarder	SplunkForwarde...	Running	Automatic	NT SERVIC...
Spot Verifier	Verifies potentia...		Manual (Trigger Start)	Local Syste...
SQL Server (SQLEXPRESS)	Provides storag...	Running	Automatic (Delayed Start)	NT Service...
SQL Server Agent (SQLEXPR...	Executes jobs, ...		Disabled	Network S...
SQL Server Browser	Provides SQL Se...		Disabled	Local Service
SQL Server CEIP service (SQ...	CEIP service for ...	Running	Automatic (Delayed Start)	NT Service...
SQL Server VSS Writer	Provides the int...		Automatic	Local Syste...
SSDP Discovery	Discovers netwo...	Running	Manual	Local Service
State Repository Service	Provides require...	Running	Automatic	Local Syste...
Still Image Acquisition Events	Launches applic...		Manual	Local Syste...
Storage Service	Provides enabli...	Running	Automatic (Delayed Start, Tr...	Local Syste...
Storage Tiers Management	Optimizes the pl...		Manual	Local Syste...

FOR SSH LOGS UPLOAD

8. Upload SSH Datalogs at Settings > Add Data > Upload Data
   a. SELECT Source [upload SSH.log, then click NEXT]



Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **SSH.log**

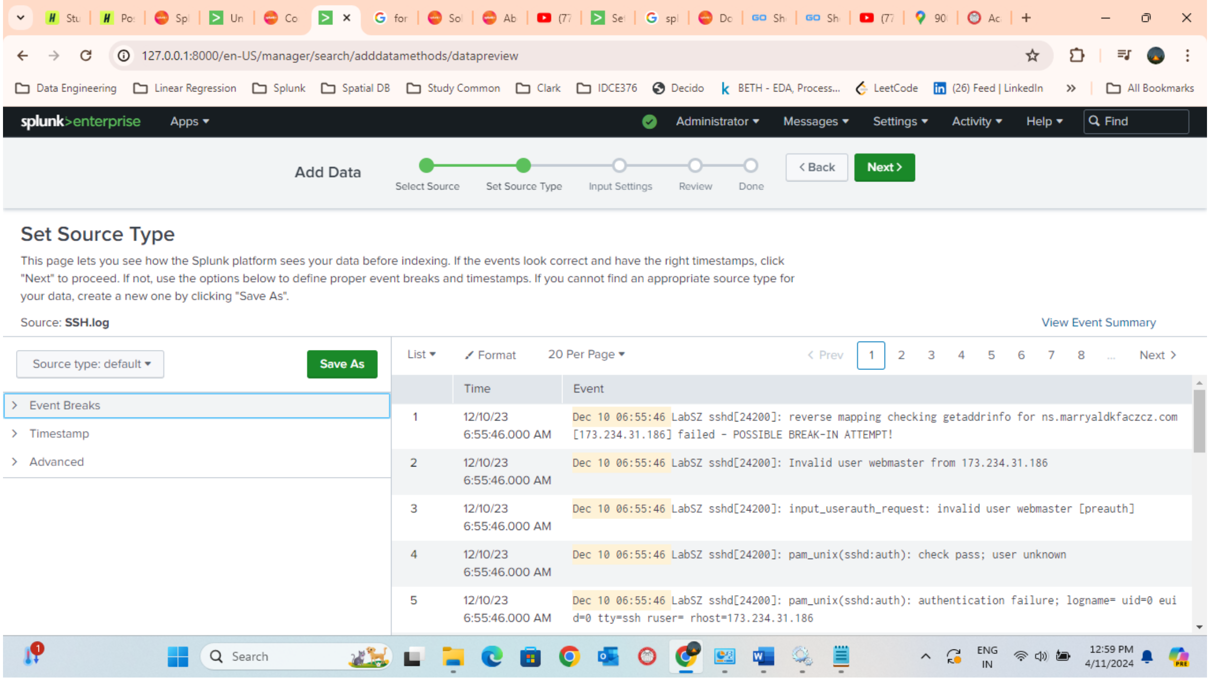
Select File

Drop your data file here

The maximum file upload size is 500 Mb

File Successfully Uploaded

   b. Set source Type [Click NEXT]



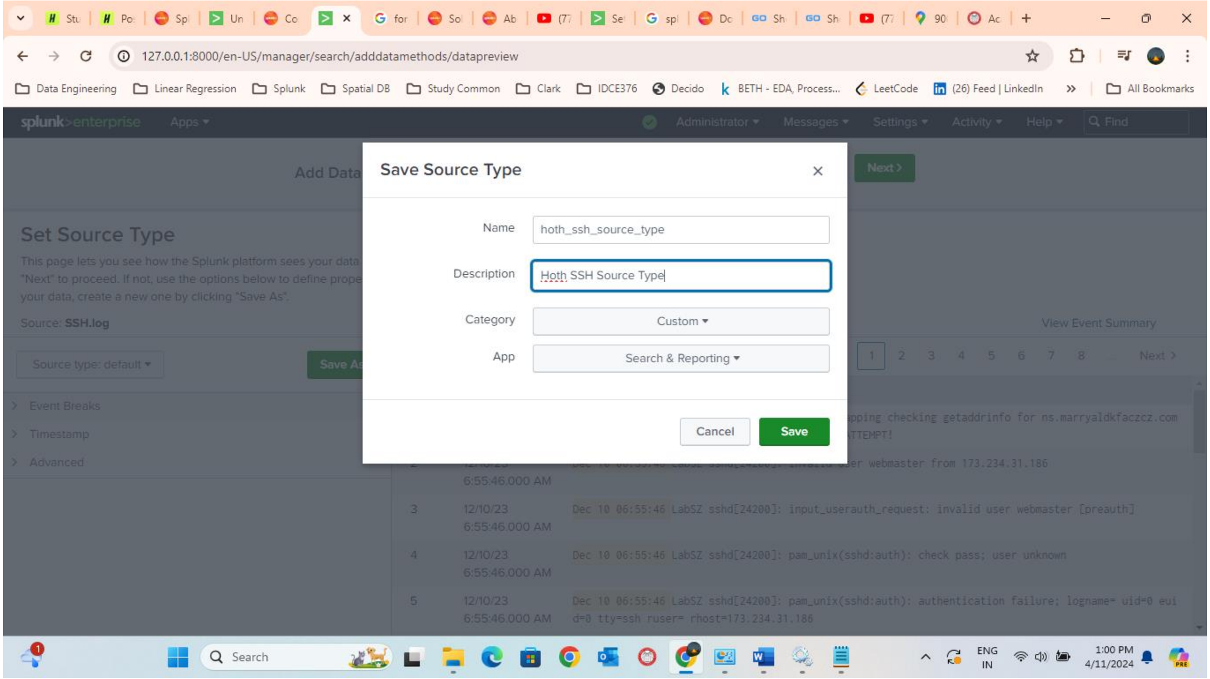
Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **SSH.log**

	Time	Event
1	12/10/23 6:55:46.000 AM	Dec 10 06:55:46 LabSZ sshd[24200]: reverse mapping checking getaddrinfo for ns.marryaldkfaczcz.com [173.234.31.186] failed - POSSIBLE BREAK-IN ATTEMPT!
2	12/10/23 6:55:46.000 AM	Dec 10 06:55:46 LabSZ sshd[24200]: Invalid user webmaster from 173.234.31.186
3	12/10/23 6:55:46.000 AM	Dec 10 06:55:46 LabSZ sshd[24200]: input_userauth_request: invalid user webmaster [preauth]
4	12/10/23 6:55:46.000 AM	Dec 10 06:55:46 LabSZ sshd[24200]: pam_unix(sshd:auth): check pass; user unknown
5	12/10/23 6:55:46.000 AM	Dec 10 06:55:46 LabSZ sshd[24200]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=173.234.31.186

   c. Fill details and click NEXT



127.0.0.1:8000/en-US/manager/search/adddatamethods/datapreview

Set Source Type

Source: SSH.log

Save Source Type

Name: hoth_ssh_source_type

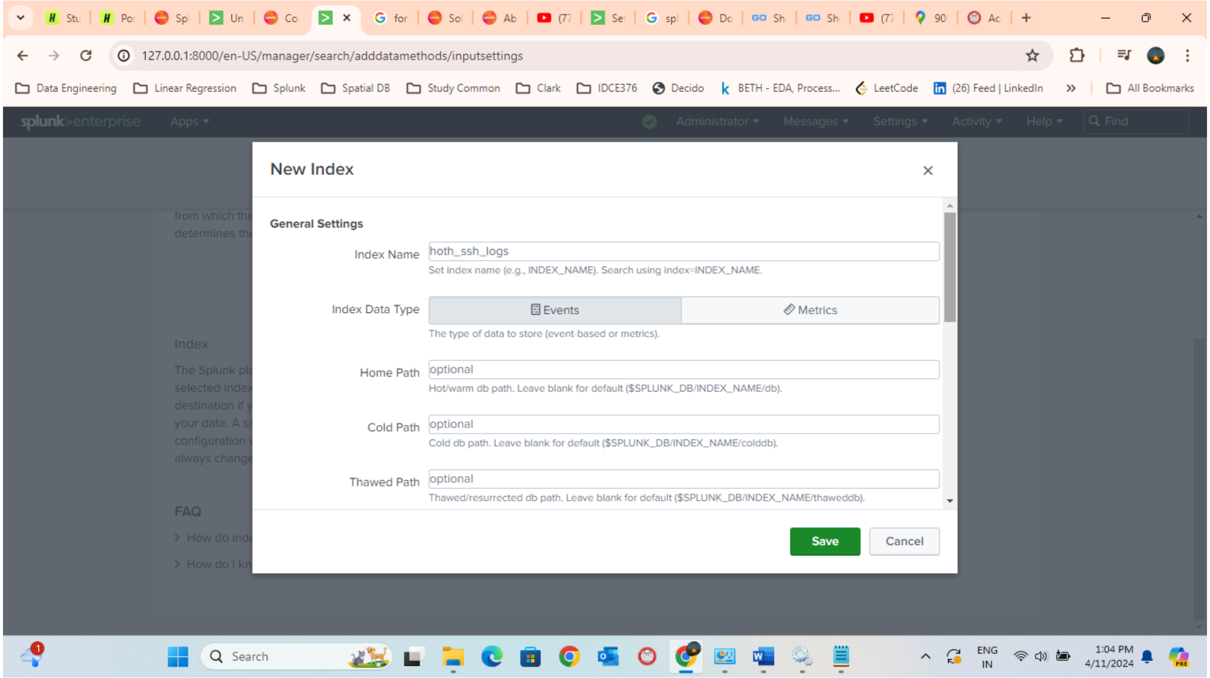
Description: Hoth SSH Source Type

Category: Custom

App: Search & Reporting

```
3  12/10/23 6:55:46.000 AM  Dec 10 06:55:46 LabSZ sshd[24200]: input_userauth_request: invalid user webmaster [preauth]
4  12/10/23 6:55:46.000 AM  Dec 10 06:55:46 LabSZ sshd[24200]: pam_unix(sshd:auth): check pass; user unknown
5  12/10/23 6:55:46.000 AM  Dec 10 06:55:46 LabSZ sshd[24200]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=173.234.31.186
```

d. Create a new Index



127.0.0.1:8000/en-US/manager/search/adddatamethods/inputsettings

New Index

General Settings

Index Name: hoth_ssh_logs
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

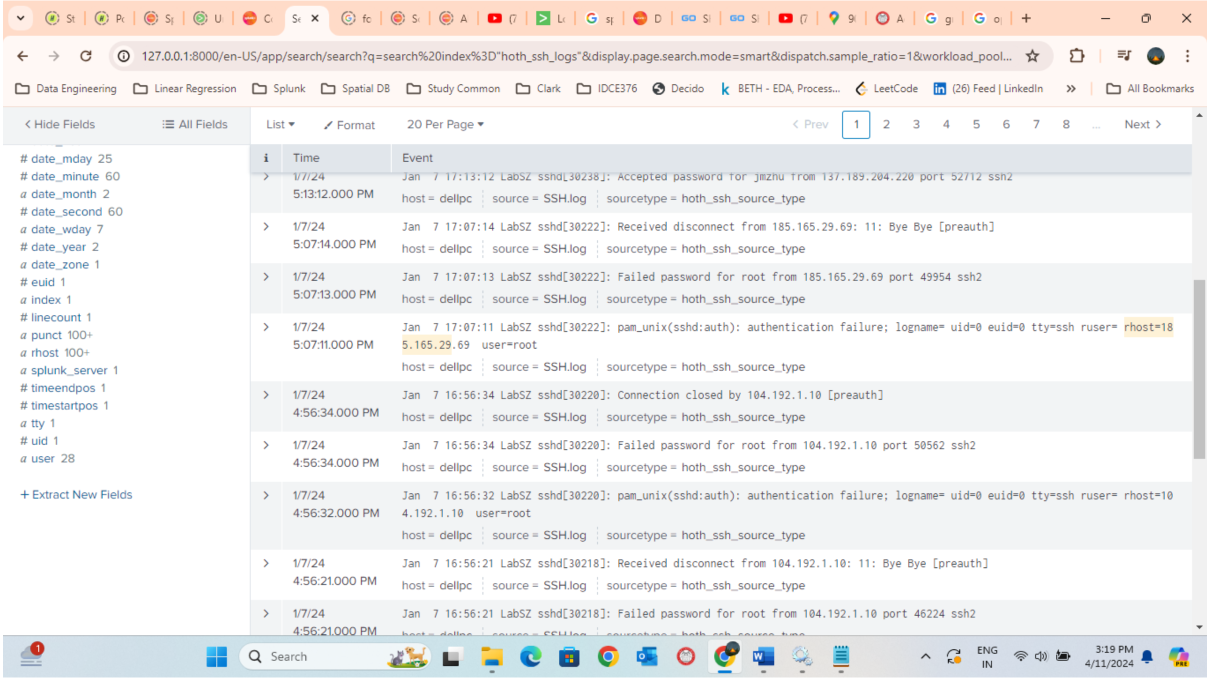
Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

e. Review and Submit.

Regular Expression Example (Extract IP Address)

9. Extract New Fields



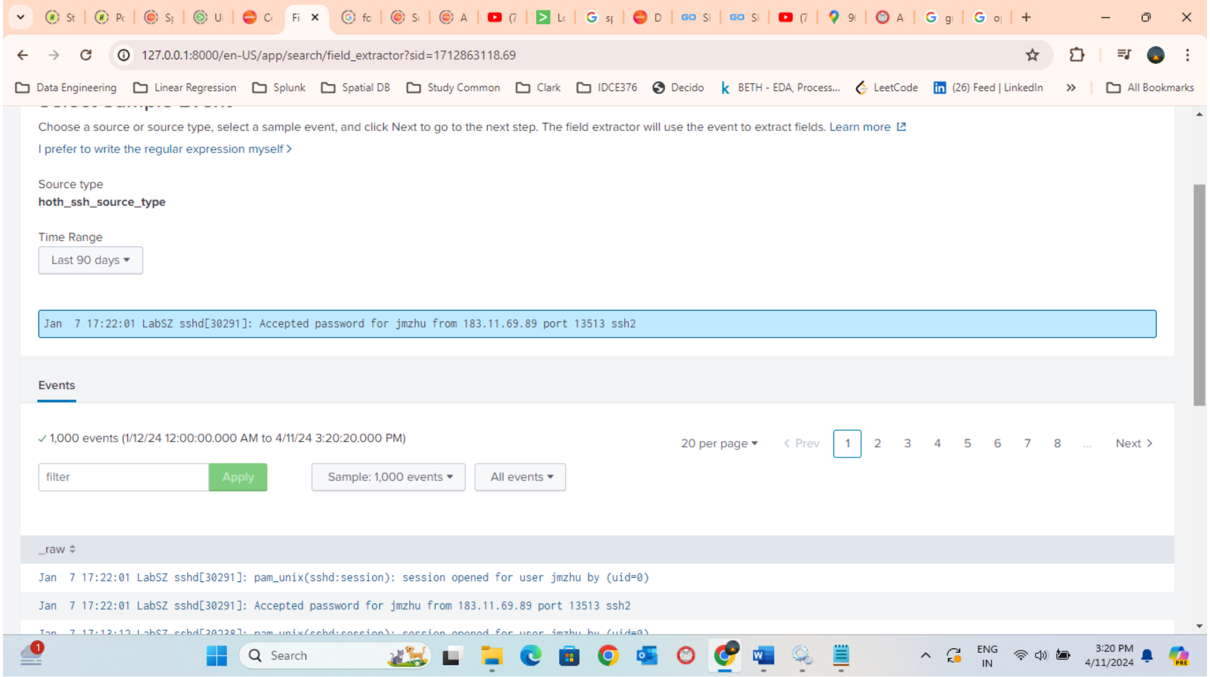
127.0.0.1:8000/en-US/app/search/search?q=search%20index%3D"hoth_ssh_logs"&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool...

- # date_mday 25
- # date_minute 60
- a date_month 2
- # date_second 60
- a date_wday 7
- # date_year 2
- a date_zone 1
- # euid 1
- a index 1
- # linecount 1
- a punct 100+
- a rhost 100+
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1
- a tty 1
- # uid 1
- a user 28

+ Extract New Fields

```
1/7/24 5:13:12.000 PM   Jan  7 17:13:12 LabSZ sshd[30238]: Accepted password for jmzhu from 137.189.204.220 port 52712 ssh2
                        host = dellpc   source = SSH.log   sourcetype = hoth_ssh_source_type
1/7/24 5:07:14.000 PM   Jan  7 17:07:14 LabSZ sshd[30222]: Received disconnect from 185.165.29.69: 11: Bye Bye [preauth]
                        host = dellpc   source = SSH.log   sourcetype = hoth_ssh_source_type
1/7/24 5:07:13.000 PM   Jan  7 17:07:13 LabSZ sshd[30222]: Failed password for root from 185.165.29.69 port 49954 ssh2
                        host = dellpc   source = SSH.log   sourcetype = hoth_ssh_source_type
1/7/24 5:07:11.000 PM   Jan  7 17:07:11 LabSZ sshd[30222]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=18
                        5.165.29.69  user=root
                        host = dellpc   source = SSH.log   sourcetype = hoth_ssh_source_type
1/7/24 4:56:34.000 PM   Jan  7 16:56:34 LabSZ sshd[30220]: Connection closed by 104.192.1.10 [preauth]
                        host = dellpc   source = SSH.log   sourcetype = hoth_ssh_source_type
1/7/24 4:56:34.000 PM   Jan  7 16:56:34 LabSZ sshd[30220]: Failed password for root from 104.192.1.10 port 50562 ssh2
                        host = dellpc   source = SSH.log   sourcetype = hoth_ssh_source_type
1/7/24 4:56:32.000 PM   Jan  7 16:56:32 LabSZ sshd[30220]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10
                        4.192.1.10  user=root
                        host = dellpc   source = SSH.log   sourcetype = hoth_ssh_source_type
1/7/24 4:56:21.000 PM   Jan  7 16:56:21 LabSZ sshd[30218]: Received disconnect from 104.192.1.10: 11: Bye Bye [preauth]
                        host = dellpc   source = SSH.log   sourcetype = hoth_ssh_source_type
1/7/24 4:56:21.000 PM   Jan  7 16:56:21 LabSZ sshd[30218]: Failed password for root from 104.192.1.10 port 46224 ssh2
```

10. Select some record with IP address click NEXT:



127.0.0.1:8000/en-US/app/search/field_extractor?sid=1712863118.69

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. Learn more

I prefer to write the regular expression myself >

Source type
hoth_ssh_source_type

Time Range
Last 90 days

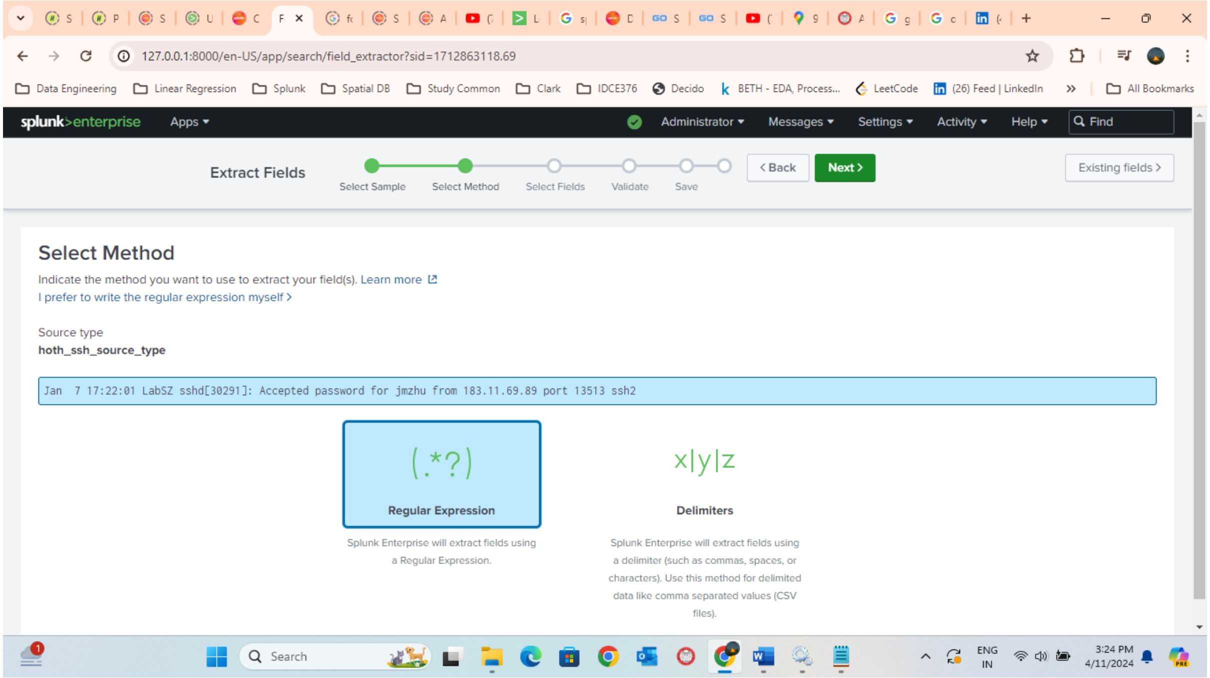
```
Jan  7 17:22:01 LabSZ sshd[30291]: Accepted password for jmzhu from 183.11.69.89 port 13513 ssh2
```

Events

✓ 1,000 events (1/12/24 12:00:00.000 AM to 4/11/24 3:20:20.000 PM)

```
_raw
Jan  7 17:22:01 LabSZ sshd[30291]: pam_unix(sshd:session): session opened for user jmzhu by (uid=0)
Jan  7 17:22:01 LabSZ sshd[30291]: Accepted password for jmzhu from 183.11.69.89 port 13513 ssh2
```

11. Select Regular Expression Option and click NEXT



Extract Fields

Select Sample — Select Method — Select Fields — Validate — Save

< Back | Next > | Existing fields >

Select Method

Indicate the method you want to use to extract your field(s). Learn more

I prefer to write the regular expression myself >

Source type
hoth_ssh_source_type

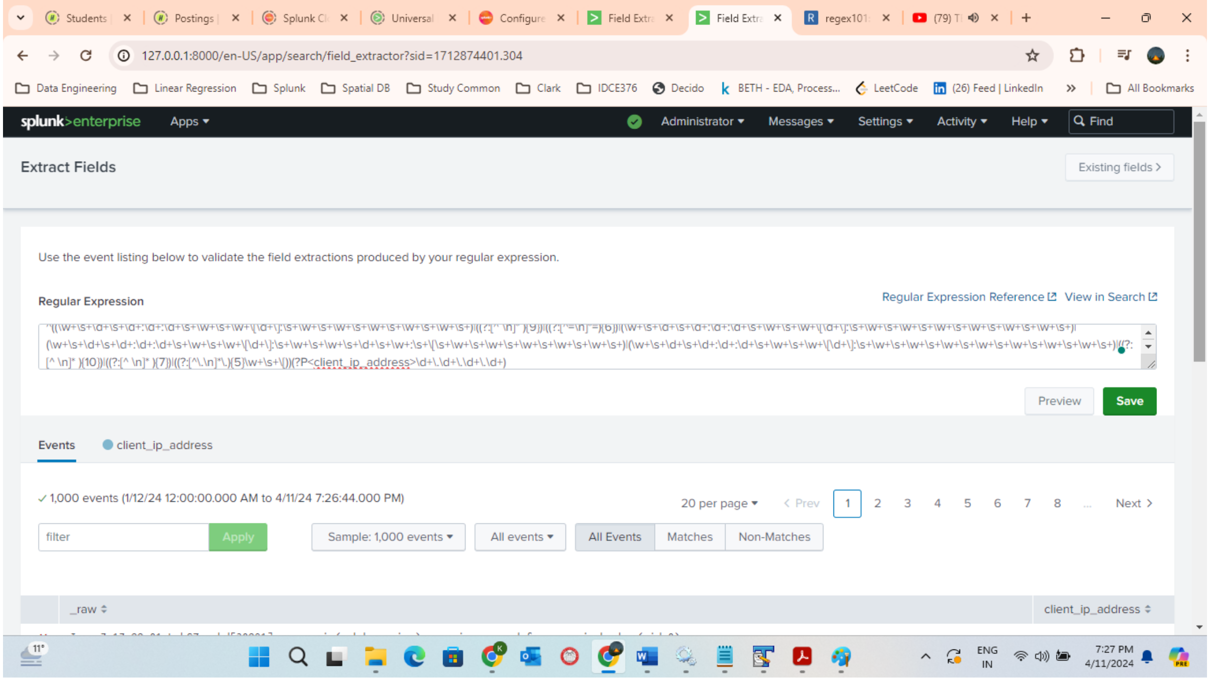
```
Jan  7 17:22:01 LabSZ sshd[30291]: Accepted password for jmzhu from 183.11.69.89 port 13513 ssh2
```

Regular Expression
Splunk Enterprise will extract fields using a Regular Expression.

Delimiters
Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

12. Click on “I prefer to write the regular expression myself” and use below regular expression:

```
^((\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\w+\[\d+\]:\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+)|((?:[^ \n]*
){9})|((?:[^=\n]*=){6})|(\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\w+\[\d+\]:\s+\w+\s+\w+\s+\w+\s+\w+\s
+\w+\s+\w+\s+)|(\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\w+\[\d+\]:\s+\w+\s+\w+\s+\d+\s+\w+:\s+\[\s
+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+)|(\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\w+\[\d+\]:\s+\w+\s+\w+
\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+)|((?:[^ \n]* ){10})|((?:[^ \n]*
){7})|((?:[^\.\n]*\.){5}\w+\s+\[))(?P<client_ip_address>\d+\.\d+\.\d+\.\d+)
```



Extract Fields

Existing fields >

Use the event listing below to validate the field extractions produced by your regular expression.

Regular Expression

Regular Expression Reference | View in Search

```
^((\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\w+\[\d+\]:\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+)|((?:[^ \n]* ){9})|((?:[^=\n]*=){6})|(\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\w+\[\d+\]:\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+)|
(\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\w+\[\d+\]:\s+\w+\s+\w+\s+\d+\s+\w+:\s+\[\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+)|(\w+\s+\d+\s+\d+:\d+:\d+\s+\w+\s+\w+\[\d+\]:\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+)|((?:
[^ \n]* ){10})|((?:[^ \n]* ){7})|((?:[^\.\n]*\.){5}\w+\s+\[))(?P<client_ip_address>\d+\.\d+\.\d+\.\d+)
```

Preview | Save

Events | client_ip_address

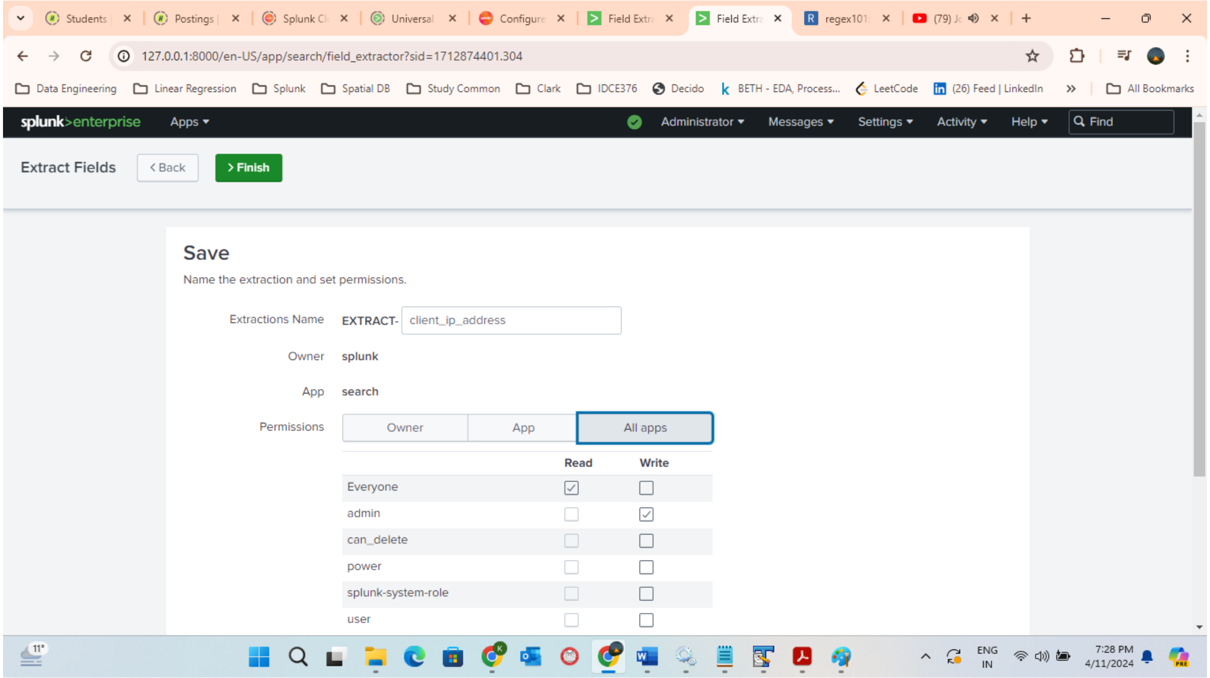
✓ 1,000 events (1/12/24 12:00:00.000 AM to 4/11/24 7:26:44.000 PM)

20 per page | < Prev | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ... | Next >

filter | Apply | Sample: 1,000 events | All events | All Events | Matches | Non-Matches

_raw | client_ip_address

13. Click on Preview and then Save after validation. Change Permissions to “All apps”:



Extract Fields

Save

Name the extraction and set permissions.

Extractions Name EXTRACT- client_ip_address

Owner splunk

App search

Permissions: Owner | App | [✓ All apps]

	Read	Write
Everyone	☑	☐
admin	☐	☑
can_delete	☐	☐
power	☐	☐
splunk-system-role	☐	☐
user	☐	☐

14. Do same for user_name. Use below regular expression:

^((.* invalid user)|(.* user)|(.*password for)|((?:[^=\n]*=){7}))(?P<user_name>\w+)