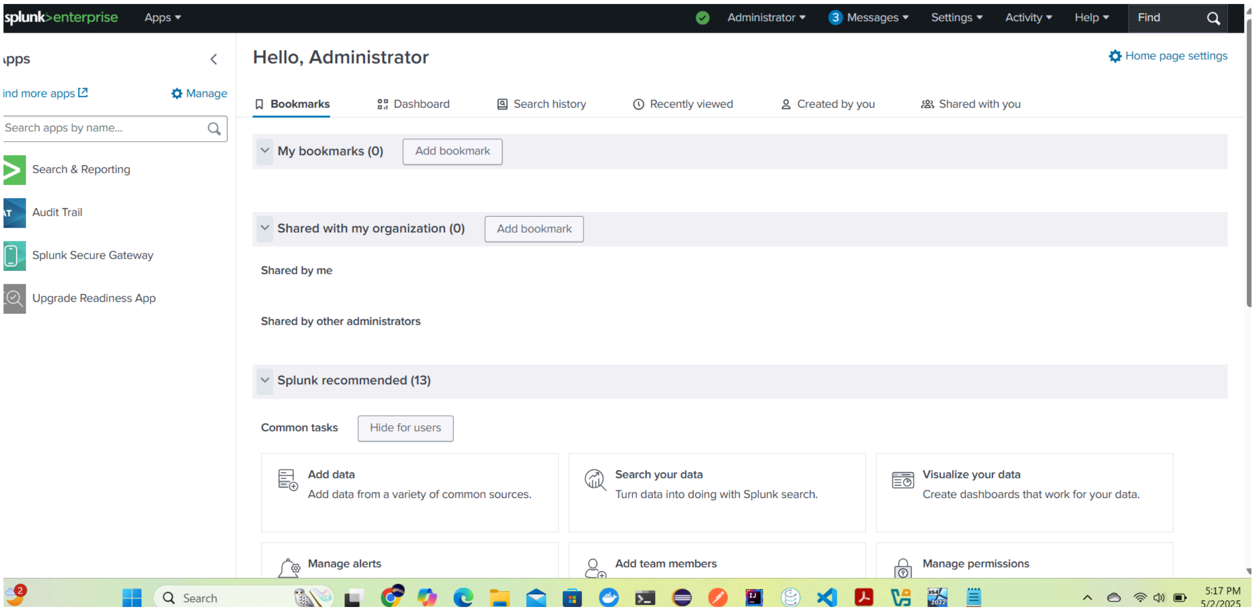
MANAGING USERS AND PERMISSIONS IN SIEM (SPLUNK)

Objective: To implement role-based access control (RBAC) in Splunk Enterprise, create roles, and manage user permissions for secure and efficient access management
Tools Used: Splunk version 9.3.1, Windows OS
Prerequisites: Splunk Enterprise should already be installed

By following these steps, I successfully implemented role-based access control (RBAC) in Splunk Enterprise. This enhances security, ensures compliance, and simplifies user permission management, enabling secure and efficient data access control.
Steps to be followed:

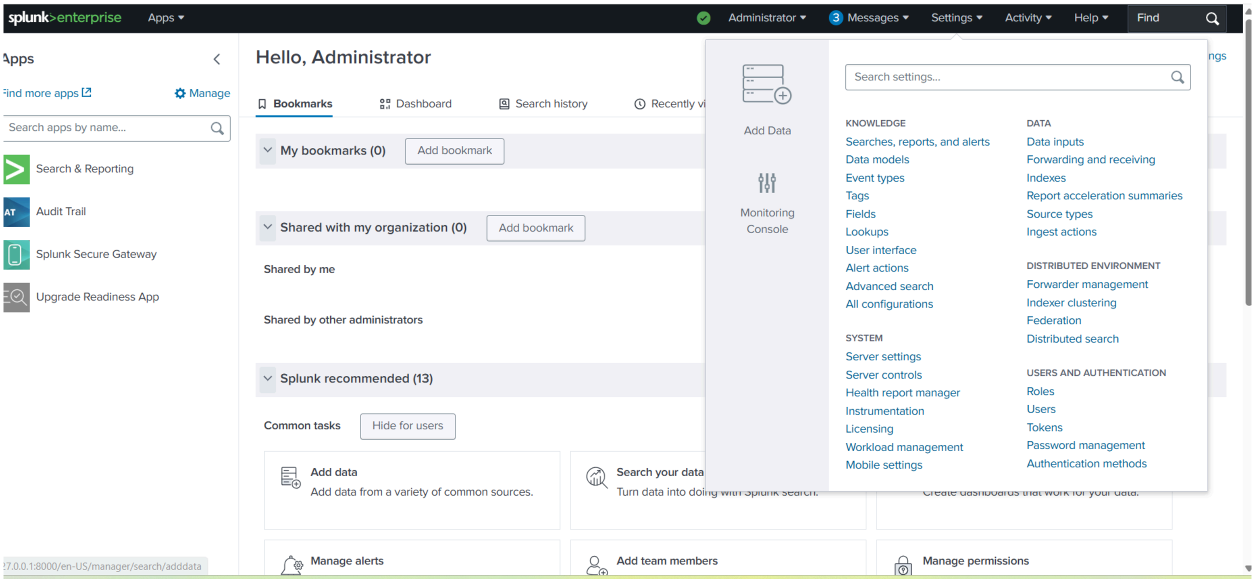
1. **Created a role**
2. **Created a new user**

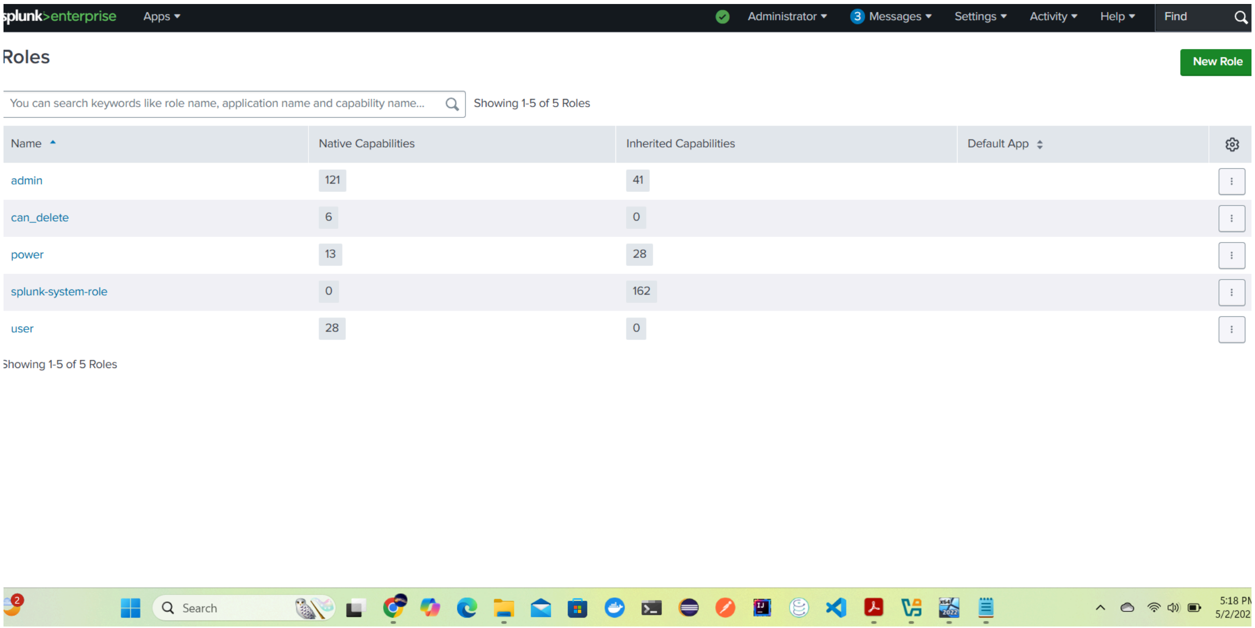


Add data from a variety of common sources.

Turn data into doing with Splunk search.

Create dashboards that work for your data.



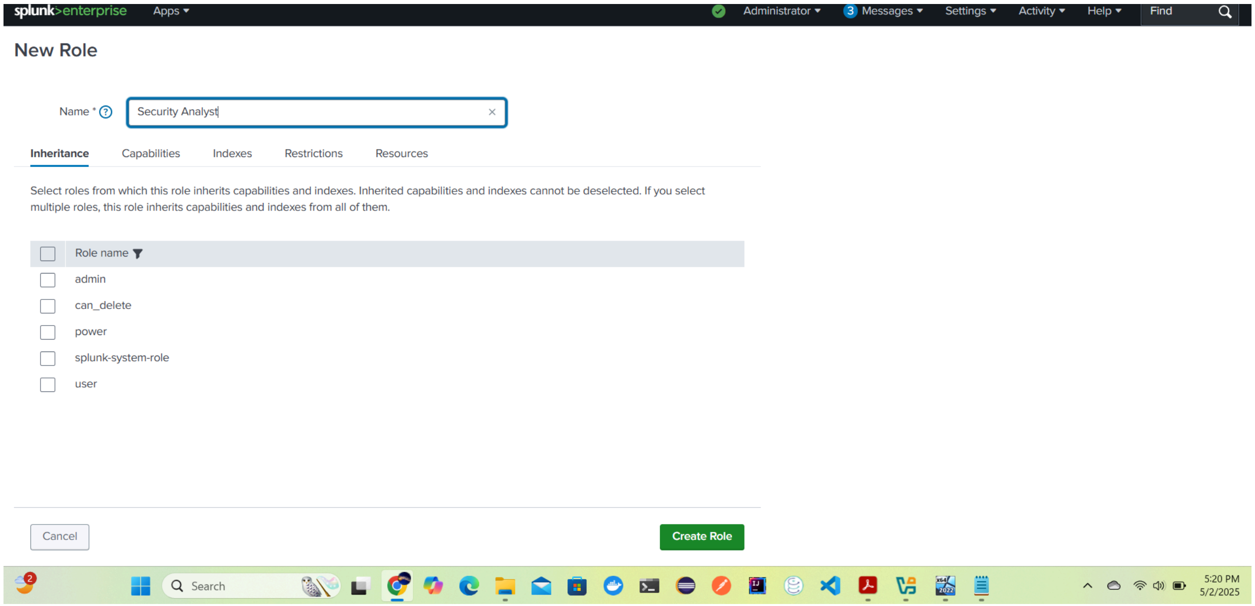


Roles

Showing 1-5 of 5 Roles

Name	Native Capabilities	Inherited Capabilities	Default App
admin	121	41	
can_delete	6	0	
power	13	28	
splunk-system-role	0	162	
user	28	0	

Showing 1-5 of 5 Roles

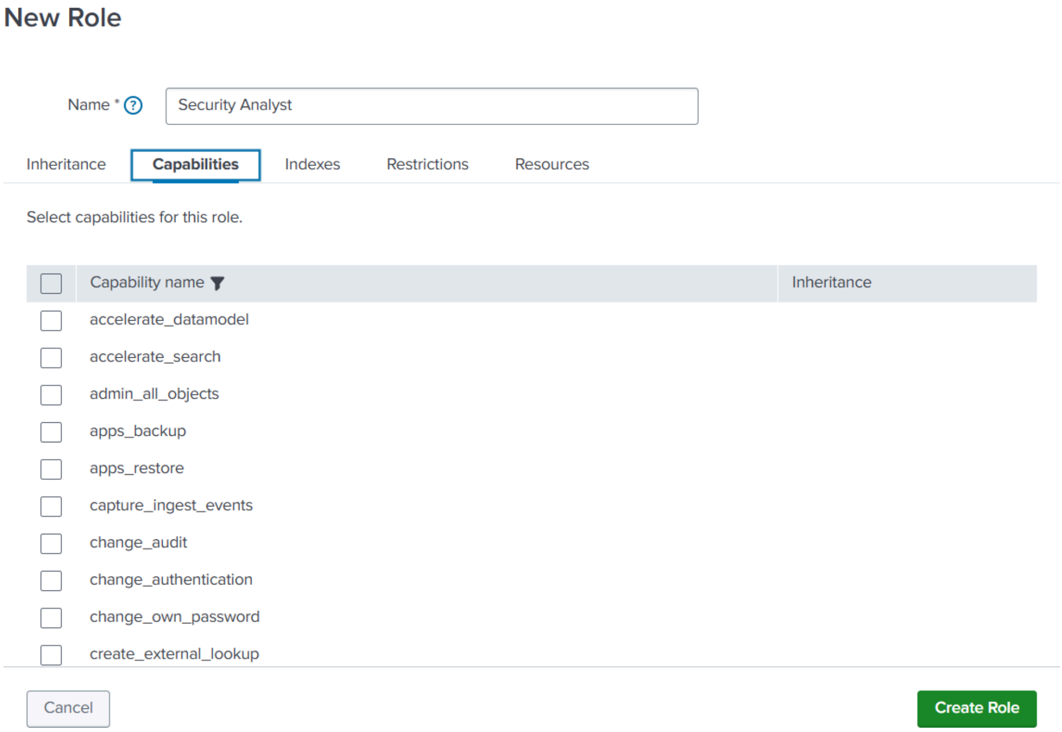


New Role

Name * ? Security Analyst

Select roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes cannot be deselected. If you select multiple roles, this role inherits capabilities and indexes from all of them.

□	Role name
□	admin
□	can_delete
□	power
□	splunk-system-role
□	user

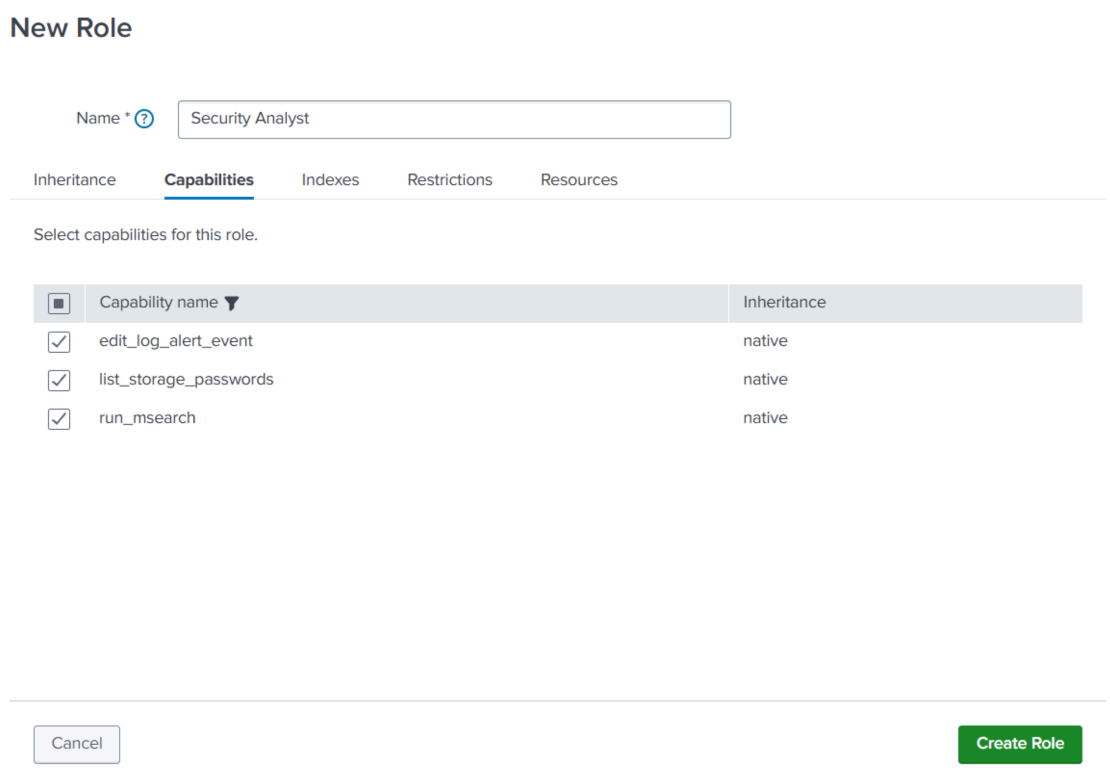


New Role

Name * ? Security Analyst

Select capabilities for this role.

□	Capability name	Inheritance
□	accelerate_datamodel	
□	accelerate_search	
□	admin_all_objects	
□	apps_backup	
□	apps_restore	
□	capture_ingest_events	
□	change_audit	
□	change_authentication	
□	change_own_password	
□	create_external_lookup	



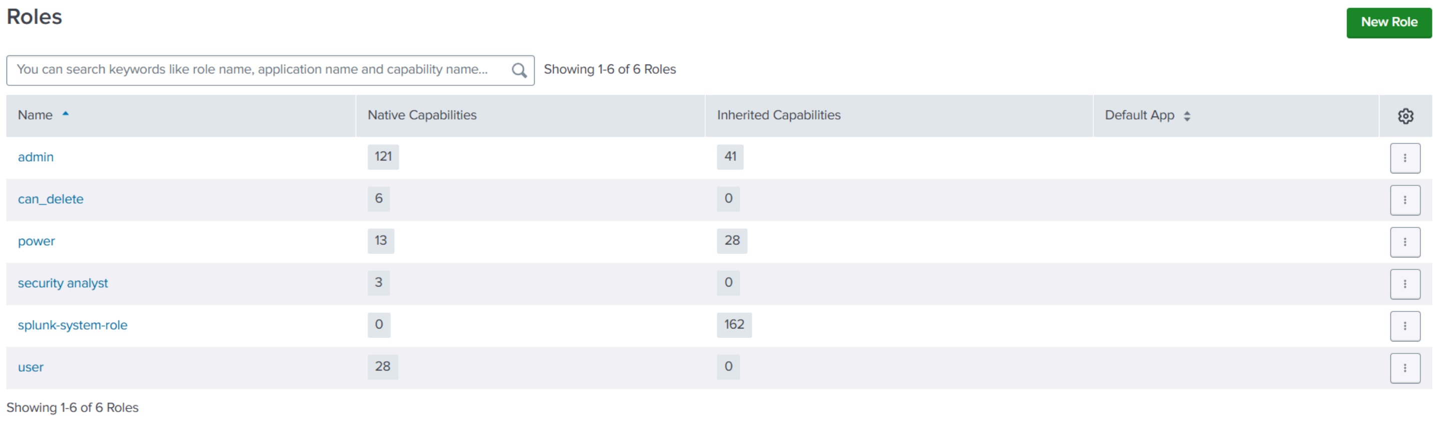
New Role

Name * ? Security Analyst

Inheritance | **Capabilities** | Indexes | Restrictions | Resources

Select capabilities for this role.

■	Capability name	Inheritance
☑	edit_log_alert_event	native
☑	list_storage_passwords	native
☑	run_msearch	native



Roles

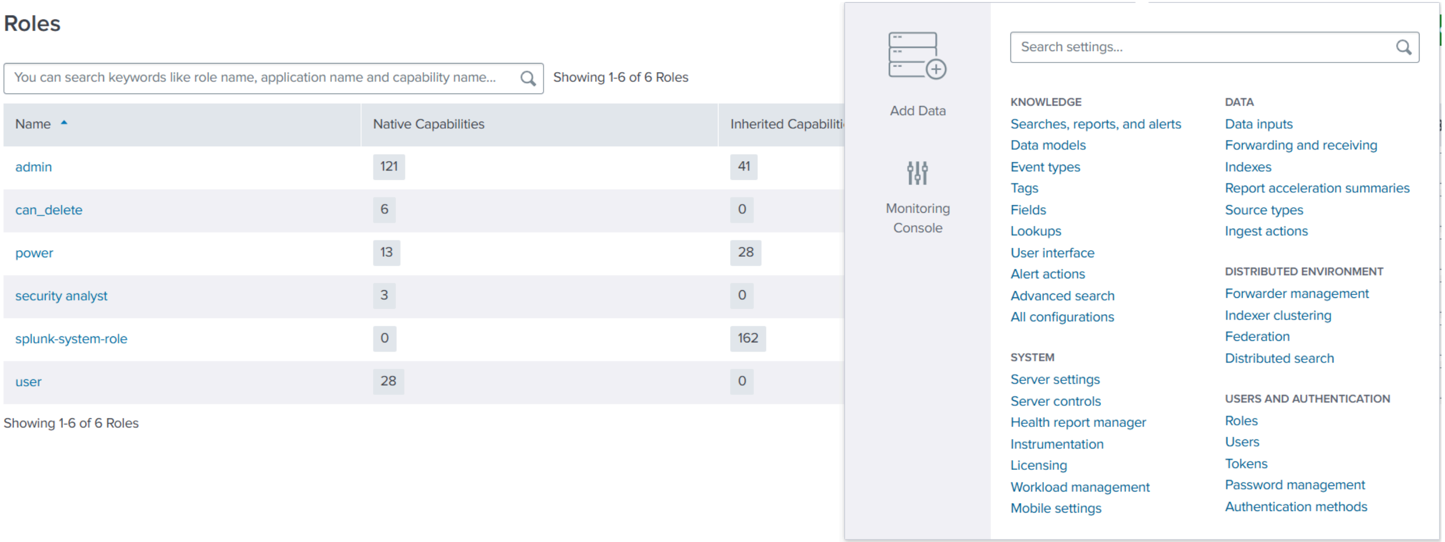
New Role
You can search keywords like role name, application name and capability name...

Showing 1-6 of 6 Roles

Name	Native Capabilities	Inherited Capabilities	Default App
admin	121	41	
can_delete	6	0	
power	13	28	
security analyst	3	0	
splunk-system-role	0	162	
user	28	0	

Showing 1-6 of 6 Roles

Step 2: Created a new user



Roles

You can search keywords like role name, application name and capability name... Showing 1-6 of 6 Roles

Name ▲	Native Capabilities	Inherited Capabiliti
admin	121	41
can_delete	6	0
power	13	28
security analyst	3	0
splunk-system-role	0	162
user	28	0

Showing 1-6 of 6 Roles

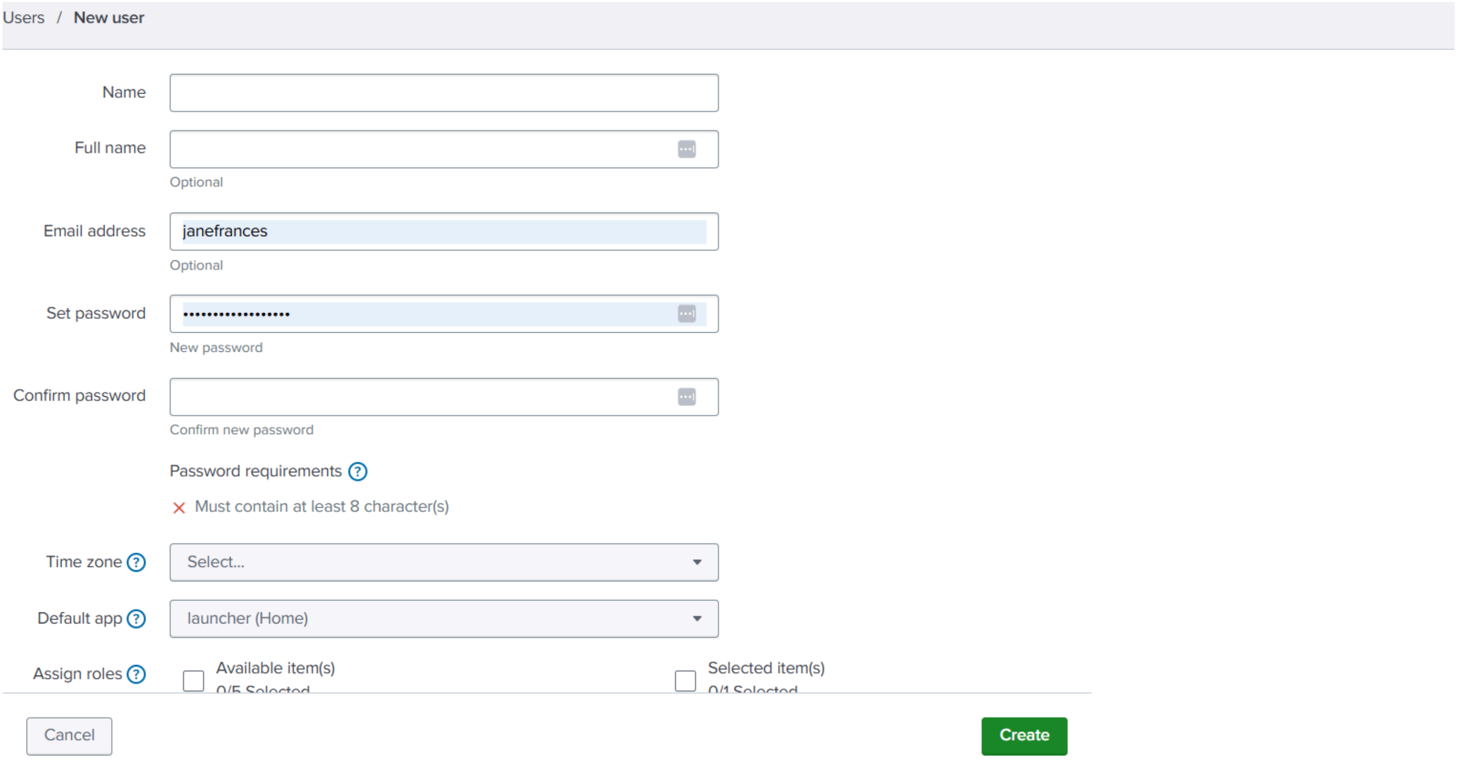
KNOWLEDGE
- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

SYSTEM
- Server settings
- Server controls
- Health report manager
- Instrumentation
- Licensing
- Workload management
- Mobile settings

DATA
- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT
- Forwarder management
- Indexer clustering
- Federation
- Distributed search

USERS AND AUTHENTICATION
- Roles
- Users
- Tokens
- Password management
- Authentication methods



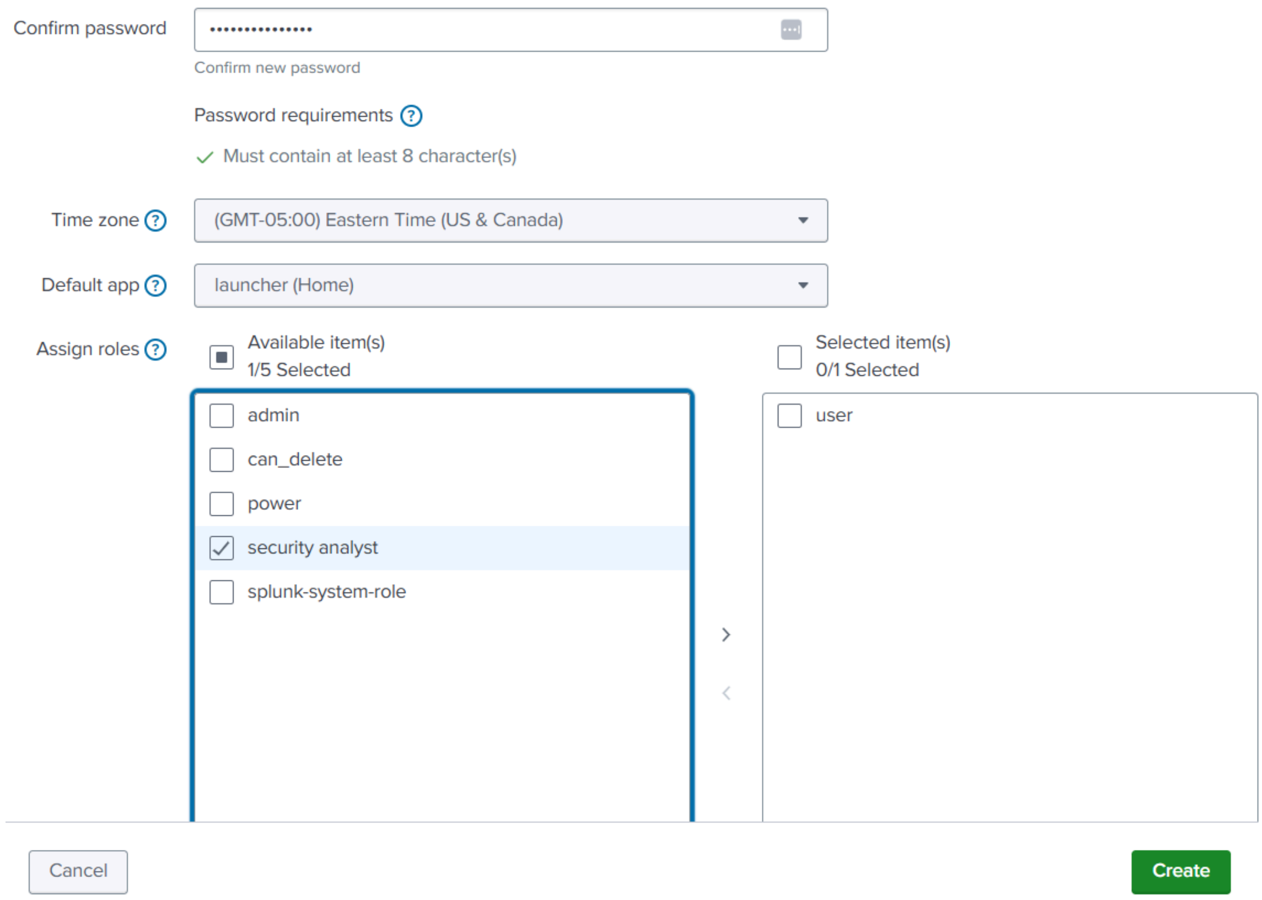
Users / **New user**

Name	
Full name	Optional
Email address	janefrances Optional
Set password	•••••••••••••••••• New password
Confirm password	Confirm new password

Password requirements ?

✕ Must contain at least 8 character(s)

Time zone ?	Select... ▾
Default app ?	launcher (Home) ▾
Assign roles ?	□ Available item(s) 0/5 Selected □ Selected item(s) 0/1 Selected



Confirm password: ••••••••••••••

Confirm new password

Password requirements ?

✓ Must contain at least 8 character(s)

Time zone ?: (GMT-05:00) Eastern Time (US & Canada)

Default app ?: launcher (Home)

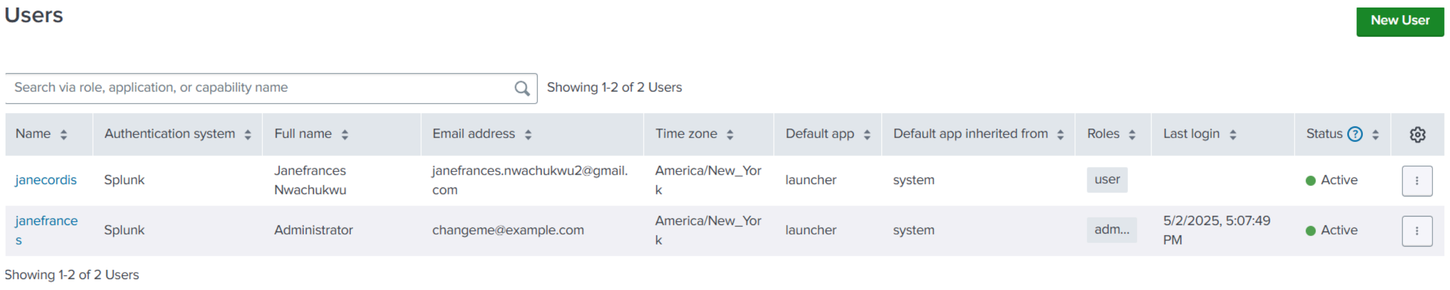
Assign roles ?

■ Available item(s) 1/5 Selected

- □ admin
- □ can_delete
- □ power
- ☑ security analyst
- □ splunk-system-role

□ Selected item(s) 0/1 Selected

- □ user



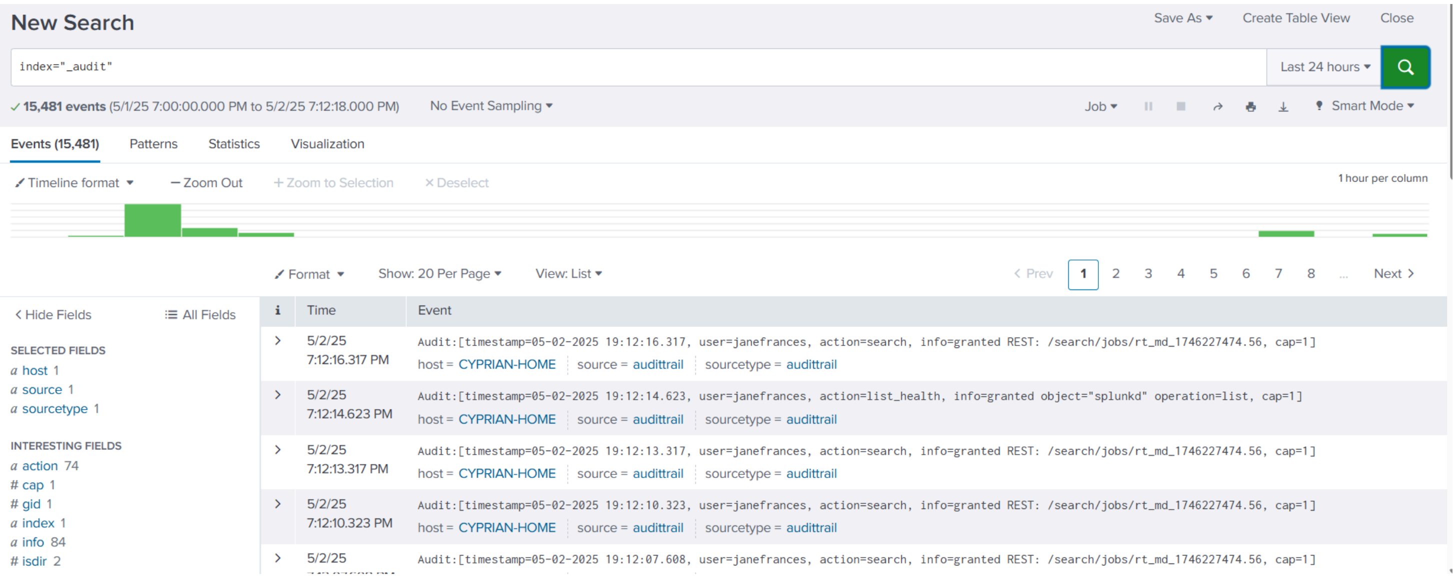
Users

Showing 1-2 of 2 Users

Name	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last login	Status	
janecordis	Splunk	Janefrances Nwachukwu	janefrances.nwachukwu2@gmail.com	America/New_York	launcher	system	user		● Active	⋮
janefrances	Splunk	Administrator	changeme@example.com	America/New_York	launcher	system	adm...	5/2/2025, 5:07:49 PM	● Active	⋮

Showing 1-2 of 2 Users

Auditing Logs of Windows and Splunk



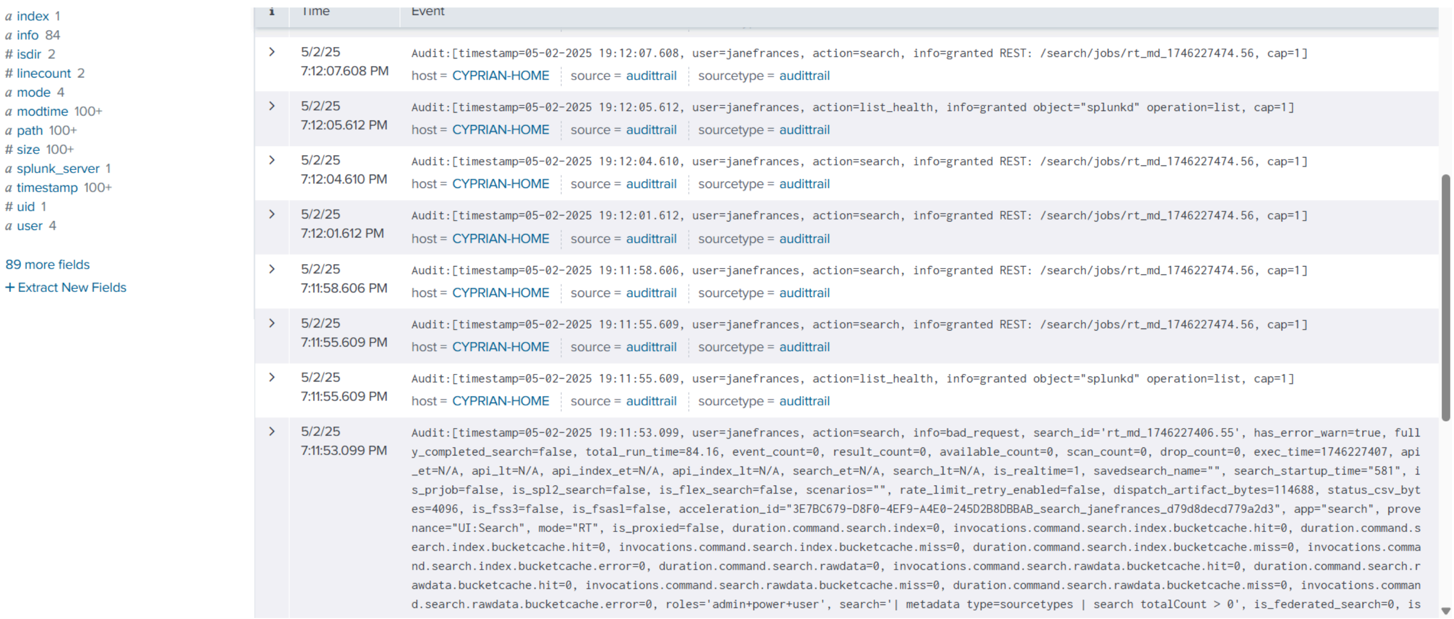
```
index="_audit"
```

✓ 15,481 events (5/1/25 7:00:00.000 PM to 5/2/25 7:12:18.000 PM)   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 74
# cap 1
# gid 1
a index 1
a info 84
# isdir 2

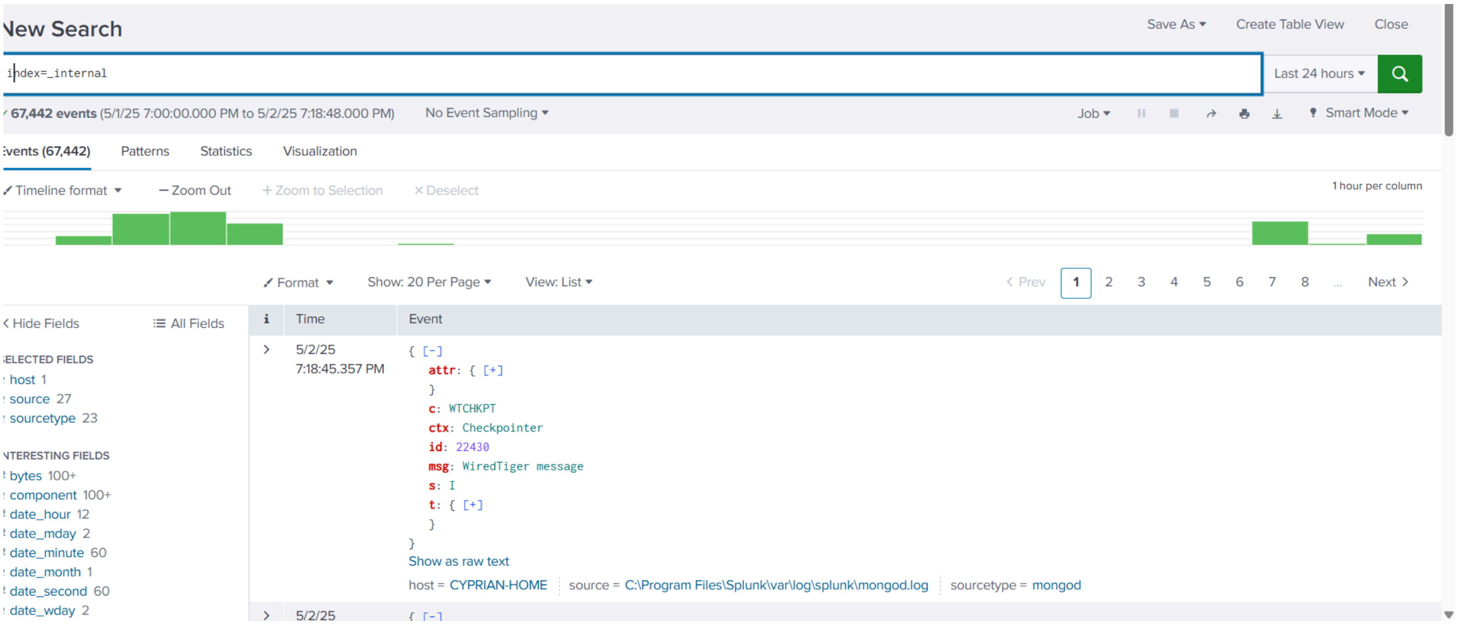
i	Time	Event
›	5/2/25 7:12:16.317 PM	Audit:[timestamp=05-02-2025 19:12:16.317, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:12:14.623 PM	Audit:[timestamp=05-02-2025 19:12:14.623, user=janefrances, action=list_health, info=granted object="splunkd" operation=list, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:12:13.317 PM	Audit:[timestamp=05-02-2025 19:12:13.317, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:12:10.323 PM	Audit:[timestamp=05-02-2025 19:12:10.323, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25	Audit:[timestamp=05-02-2025 19:12:07.608, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1]



a index 1
a info 84
# isdir 2
# linecount 2
a mode 4
a modtime 100+
a path 100+
# size 100+
a splunk_server 1
a timestamp 100+
# uid 1
a user 4

89 more fields
+ Extract New Fields

i	Time	Event
›	5/2/25 7:12:07.608 PM	Audit:[timestamp=05-02-2025 19:12:07.608, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:12:05.612 PM	Audit:[timestamp=05-02-2025 19:12:05.612, user=janefrances, action=list_health, info=granted object="splunkd" operation=list, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:12:04.610 PM	Audit:[timestamp=05-02-2025 19:12:04.610, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:12:01.612 PM	Audit:[timestamp=05-02-2025 19:12:01.612, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:11:58.606 PM	Audit:[timestamp=05-02-2025 19:11:58.606, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:11:55.609 PM	Audit:[timestamp=05-02-2025 19:11:55.609, user=janefrances, action=search, info=granted REST: /search/jobs/rt_md_1746227474.56, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:11:55.609 PM	Audit:[timestamp=05-02-2025 19:11:55.609, user=janefrances, action=list_health, info=granted object="splunkd" operation=list, cap=1] host = CYPRIAN-HOME source = audittrail sourcetype = audittrail
›	5/2/25 7:11:53.099 PM	Audit:[timestamp=05-02-2025 19:11:53.099, user=janefrances, action=search, info=bad_request, search_id='rt_md_1746227406.55', has_error_warn=true, fully_completed_search=false, total_run_time=84.16, event_count=0, result_count=0, available_count=0, scan_count=0, drop_count=0, exec_time=1746227407, api_et=N/A, api_lt=N/A, api_index_et=N/A, api_index_lt=N/A, search_et=N/A, search_lt=N/A, is_realtime=1, savedsearch_name="", search_startup_time="581", is_prjob=false, is_spl2_search=false, is_flex_search=false, scenarios="", rate_limit_retry_enabled=false, dispatch_artifact_bytes=114688, status_csv_bytes=4096, is_fss3=false, is_fsasl=false, acceleration_id="3E7BC679-D8F0-4EF9-A4E0-245D2B8DBBAB_search_janefrances_d79d8decd779a2d3", app="search", provenance="UI:Search", mode="RT", is_proxied=false, duration.command.search.index=0, invocations.command.search.index.bucketcache.hit=0, duration.command.search.index.bucketcache.hit=0, invocations.command.search.index.bucketcache.miss=0, duration.command.search.index.bucketcache.miss=0, invocations.command.search.index.bucketcache.error=0, duration.command.search.rawdata=0, invocations.command.search.rawdata.bucketcache.hit=0, duration.command.search.rawdata.bucketcache.hit=0, invocations.command.search.rawdata.bucketcache.miss=0, duration.command.search.rawdata.bucketcache.miss=0, invocations.command.search.rawdata.bucketcache.error=0, roles='admin+power+user', search='| metadata type=sourcetypes | search totalCount > 0', is_federated_search=0, is



```
index=_internal
```

67,442 events (5/1/25 7:00:00.000 PM to 5/2/25 7:18:48.000 PM)

SELECTED FIELDS
- host 1
- source 27
- sourcetype 23

INTERESTING FIELDS
- bytes 100+
- component 100+
- date_hour 12
- date_mday 2
- date_minute 60
- date_month 1
- date_second 60
- date_wday 2

5/2/25 7:18:45.357 PM

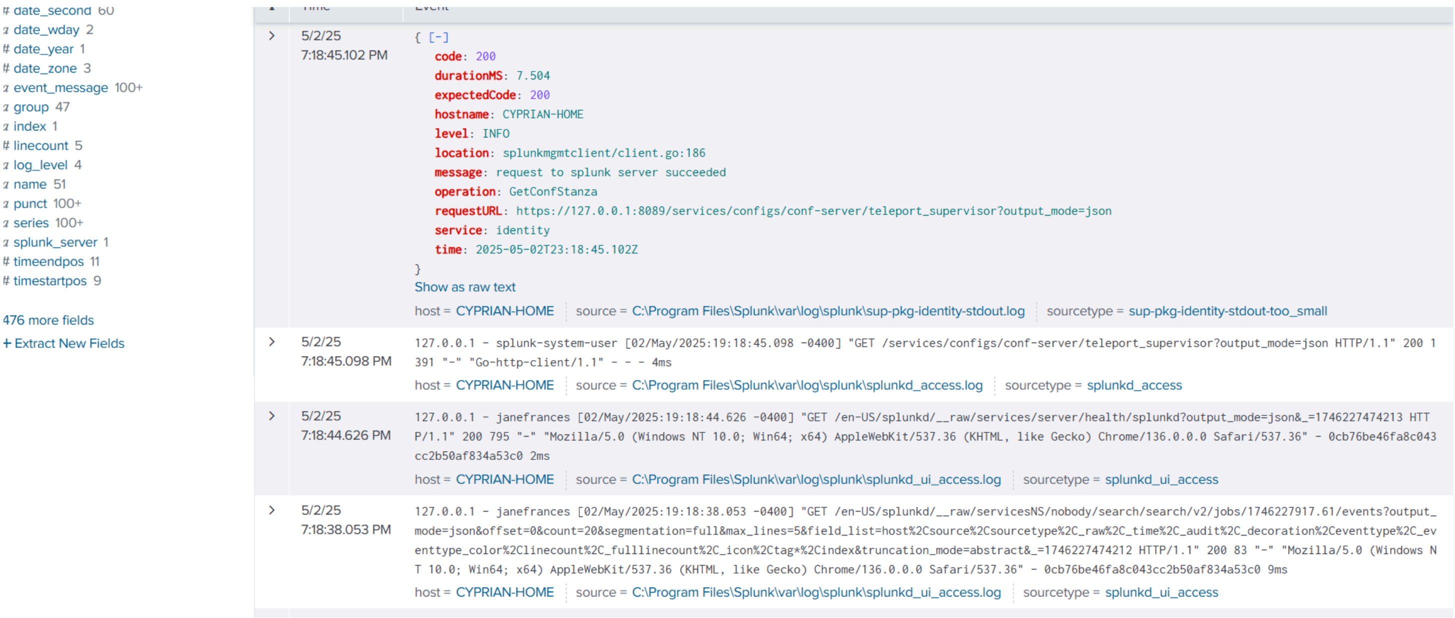
```
{ [-]
   attr: { [+]
   }
   c: WTCHKPT
   ctx: Checkpointer
   id: 22430
   msg: WiredTiger message
   s: I
   t: { [+]
   }
}
```

Show as raw text

host = CYPRIAN-HOME | source = C:\Program Files\Splunk\var\log\splunk\mongod.log | sourcetype = mongod

5/2/25

```
{ [-]
```



- date_second 60
- date_wday 2
- date_year 1
- date_zone 3
- event_message 100+
- group 47
- index 1
- linecount 5
- log_level 4
- name 51
- punct 100+
- series 100+
- splunk_server 1
- timeendpos 11
- timestartpos 9

476 more fields

+ Extract New Fields

5/2/25 7:18:45.102 PM

```
{ [-]
   code: 200
   durationMS: 7.504
   expectedCode: 200
   hostname: CYPRIAN-HOME
   level: INFO
   location: splunkmgmtclient/client.go:186
   message: request to splunk server succeeded
   operation: GetConfStanza
   requestURL: https://127.0.0.1:8089/services/configs/conf-server/teleport_supervisor?output_mode=json
   service: identity
   time: 2025-05-02T23:18:45.102Z
}
```

Show as raw text

host = CYPRIAN-HOME | source = C:\Program Files\Splunk\var\log\splunk\sup-pkg-identity-stdout.log | sourcetype = sup-pkg-identity-stdout-too_small

5/2/25 7:18:45.098 PM

```
127.0.0.1 - splunk-system-user [02/May/2025:19:18:45.098 -0400] "GET /services/configs/conf-server/teleport_supervisor?output_mode=json HTTP/1.1" 200 1
391 "-" "Go-http-client/1.1" - - - 4ms
```

host = CYPRIAN-HOME | source = C:\Program Files\Splunk\var\log\splunk\splunkd_access.log | sourcetype = splunkd_access

5/2/25 7:18:44.626 PM

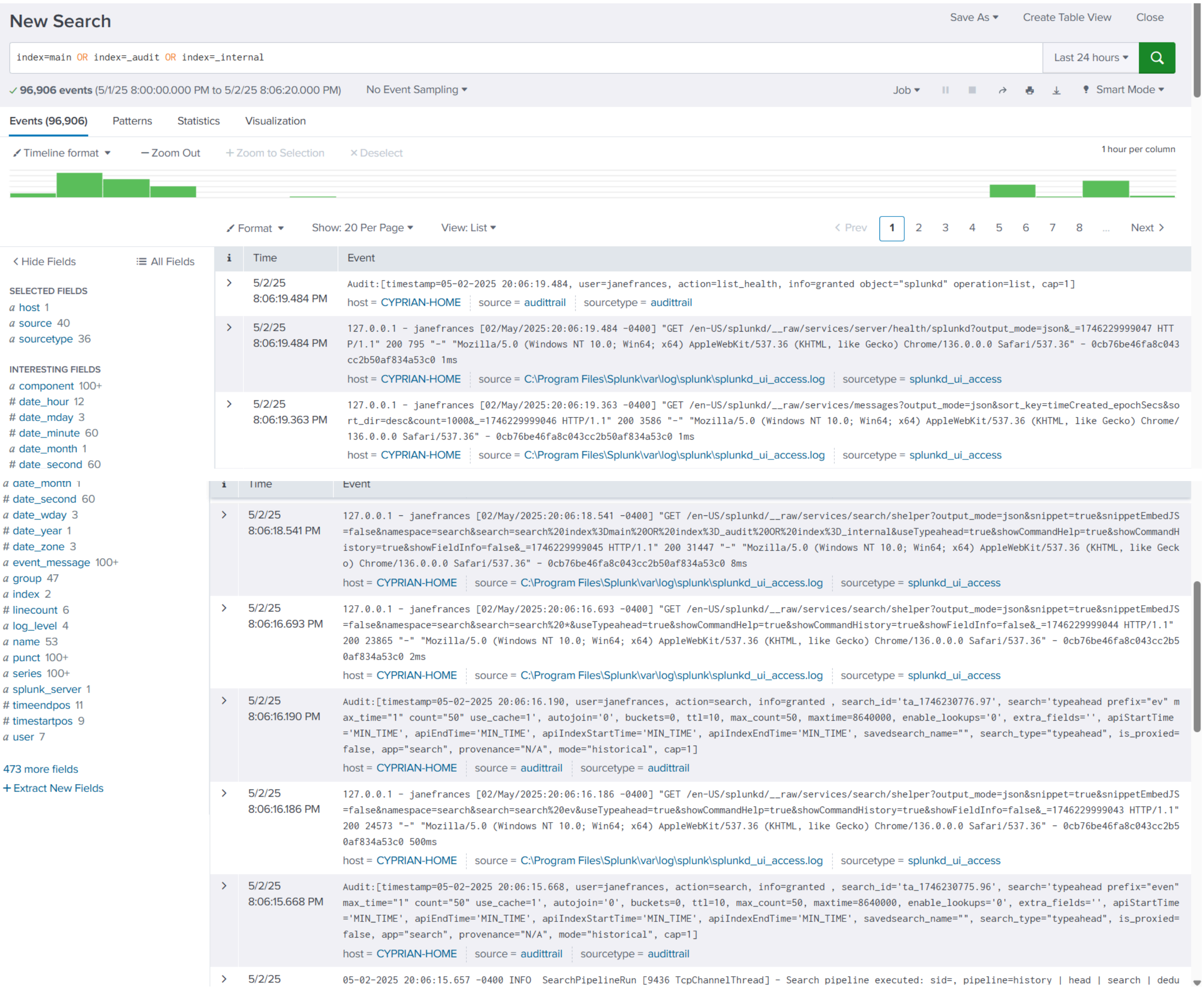
```
127.0.0.1 - janefrances [02/May/2025:19:18:44.626 -0400] "GET /en-US/splunkd/__raw/services/server/health/splunkd?output_mode=json&_=1746227474213 HTT
P/1.1" 200 795 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" - 0cb76be46fa8c043
cc2b50af834a53c0 2ms
```

host = CYPRIAN-HOME | source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log | sourcetype = splunkd_ui_access

5/2/25 7:18:38.053 PM

```
127.0.0.1 - janefrances [02/May/2025:19:18:38.053 -0400] "GET /en-US/splunkd/__raw/servicesNS/nobody/search/search/v2/jobs/1746227917.61/events?output_
mode=json&offset=0&count=20&segmentation=full&max_lines=5&field_list=host%2Csource%2Csourcetype%2C_raw%2C_time%2C_audit%2C_decoration%2Ceventtype%2C_ev
enttype_color%2Clinecount%2C_fulllinecount%2C_icon%2Ctag*%2Cindex&truncation_mode=abstract&_=1746227474212 HTTP/1.1" 200 83 "-" "Mozilla/5.0 (Windows N
T 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" - 0cb76be46fa8c043cc2b50af834a53c0 9ms
```

host = CYPRIAN-HOME | source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log | sourcetype = splunkd_ui_access



```
index=main OR index=_audit OR index=_internal
```

✓ **96,906 events** (5/1/25 8:00:00.000 PM to 5/2/25 8:06:20.000 PM)

SELECTED FIELDS

- a host 1
- a source 40
- a sourcetype 36

INTERESTING FIELDS

- a component 100+
- # date_hour 12
- # date_mday 3
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 3
- # date_year 1
- # date_zone 3
- a event_message 100+
- a group 47
- a index 2
- # linecount 6
- a log_level 4
- a name 53
- a punct 100+
- a series 100+
- a splunk_server 1
- # timeendpos 11
- # timestartpos 9
- a user 7

473 more fields

+ Extract New Fields

i	Time	Event

›	5/2/25
	8:06:19.484 PM
		`Audit:[timestamp=05-02-2025 20:06:19.484, user=janefrances, action=list_health, info=granted object="splunkd" operation=list, cap=1]`
		host = CYPRIAN-HOME source = audittrail sourcetype = audittrail

›	5/2/25
	8:06:19.484 PM
		`127.0.0.1 - janefrances [02/May/2025:20:06:19.484 -0400] "GET /en-US/splunkd/__raw/services/server/health/splunkd?output_mode=json&_=1746229999047 HTTP/1.1" 200 795 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" - 0cb76be46fa8c043cc2b50af834a53c0 1ms`
		host = CYPRIAN-HOME source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access

›	5/2/25
	8:06:19.363 PM
		`127.0.0.1 - janefrances [02/May/2025:20:06:19.363 -0400] "GET /en-US/splunkd/__raw/services/messages?output_mode=json&sort_key=timeCreated_epochSecs&sort_dir=desc&count=1000&_=1746229999046 HTTP/1.1" 200 3586 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" - 0cb76be46fa8c043cc2b50af834a53c0 1ms`
		host = CYPRIAN-HOME source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access

›	5/2/25
	8:06:18.541 PM
		`127.0.0.1 - janefrances [02/May/2025:20:06:18.541 -0400] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search%20index%3Dmain%20OR%20index%3D_audit%20OR%20index%3D_internal&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1746229999045 HTTP/1.1" 200 31447 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" - 0cb76be46fa8c043cc2b50af834a53c0 8ms`
		host = CYPRIAN-HOME source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access

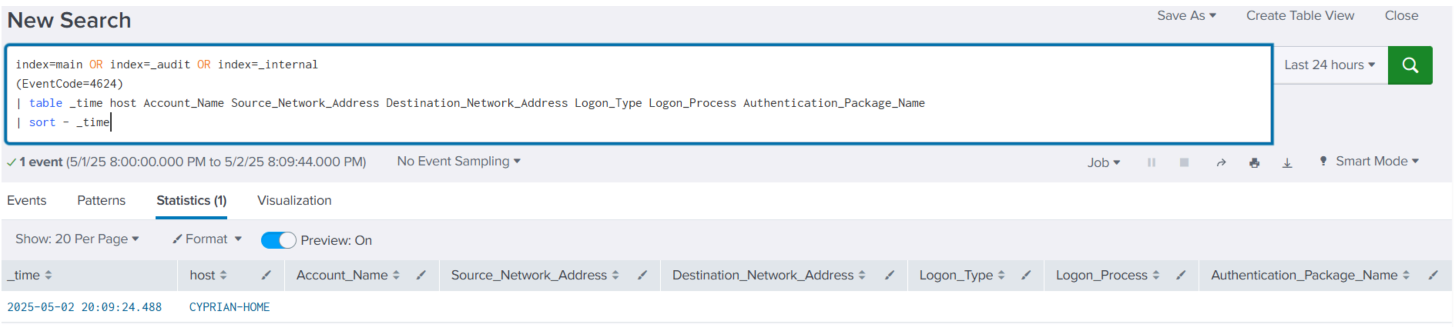
›	5/2/25
	8:06:16.693 PM
		`127.0.0.1 - janefrances [02/May/2025:20:06:16.693 -0400] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search%20*&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1746229999044 HTTP/1.1" 200 23865 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" - 0cb76be46fa8c043cc2b50af834a53c0 2ms`
		host = CYPRIAN-HOME source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access

›	5/2/25
	8:06:16.190 PM
		`Audit:[timestamp=05-02-2025 20:06:16.190, user=janefrances, action=search, info=granted , search_id='ta_1746230776.97', search='typeahead prefix="ev" max_time="1" count="50" use_cache=1', autojoin='0', buckets=0, ttl=10, max_count=50, maxtime=8640000, enable_lookups='0', extra_fields='', apiStartTime='MIN_TIME', apiEndTime='MIN_TIME', apiIndexStartTime='MIN_TIME', apiIndexEndTime='MIN_TIME', savedsearch_name="", search_type="typeahead", is_proxied=false, app="search", provenance="N/A", mode="historical", cap=1]`
		host = CYPRIAN-HOME source = audittrail sourcetype = audittrail

›	5/2/25
	8:06:16.186 PM
		`127.0.0.1 - janefrances [02/May/2025:20:06:16.186 -0400] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search%20ev&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1746229999043 HTTP/1.1" 200 24573 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36" - 0cb76be46fa8c043cc2b50af834a53c0 500ms`
		host = CYPRIAN-HOME source = C:\Program Files\Splunk\var\log\splunk\splunkd_ui_access.log sourcetype = splunkd_ui_access

›	5/2/25
	8:06:15.668 PM
		`Audit:[timestamp=05-02-2025 20:06:15.668, user=janefrances, action=search, info=granted , search_id='ta_1746230775.96', search='typeahead prefix="even" max_time="1" count="50" use_cache=1', autojoin='0', buckets=0, ttl=10, max_count=50, maxtime=8640000, enable_lookups='0', extra_fields='', apiStartTime='MIN_TIME', apiEndTime='MIN_TIME', apiIndexStartTime='MIN_TIME', apiIndexEndTime='MIN_TIME', savedsearch_name="", search_type="typeahead", is_proxied=false, app="search", provenance="N/A", mode="historical", cap=1]`
		host = CYPRIAN-HOME source = audittrail sourcetype = audittrail

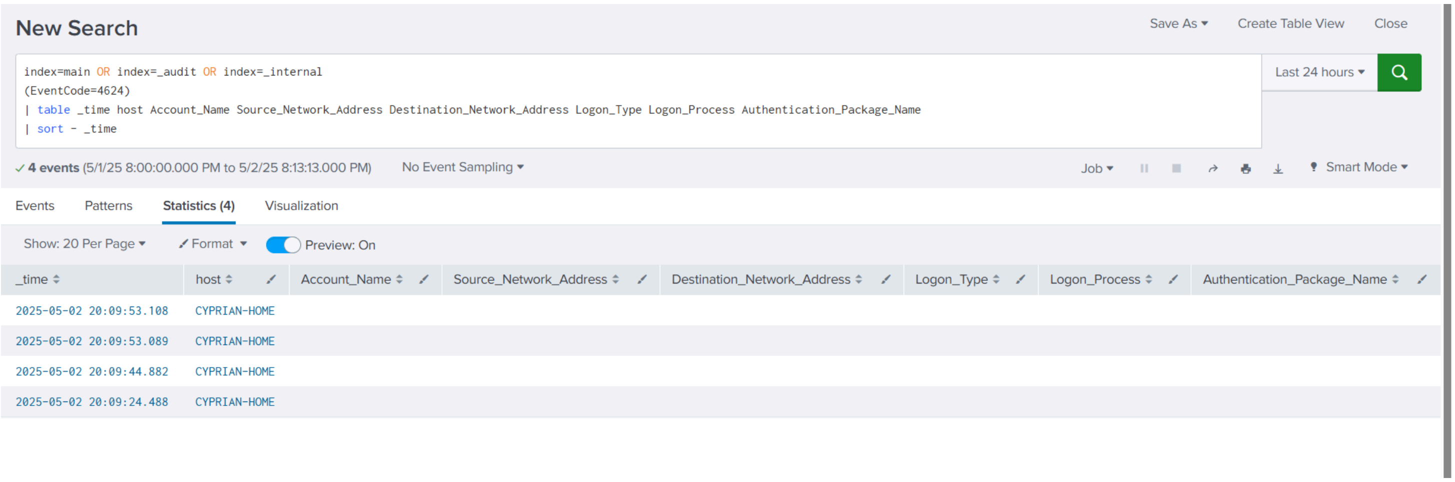
›	5/2/25	`05-02-2025 20:06:15.657 -0400 INFO  SearchPipelineRun [9436 TcpChannelThread] - Search pipeline executed: sid=, pipeline=history | head | search | dedu`



```
index=main OR index=_audit OR index=_internal
(EventCode=4624)
| table _time host Account_Name Source_Network_Address Destination_Network_Address Logon_Type Logon_Process Authentication_Package_Name
| sort - _time
```

✓ **1 event** (5/1/25 8:00:00.000 PM to 5/2/25 8:09:44.000 PM)

_time	host	Account_Name	Source_Network_Address	Destination_Network_Address	Logon_Type	Logon_Process	Authentication_Package_Name
2025-05-02 20:09:24.488	CYPRIAN-HOME						

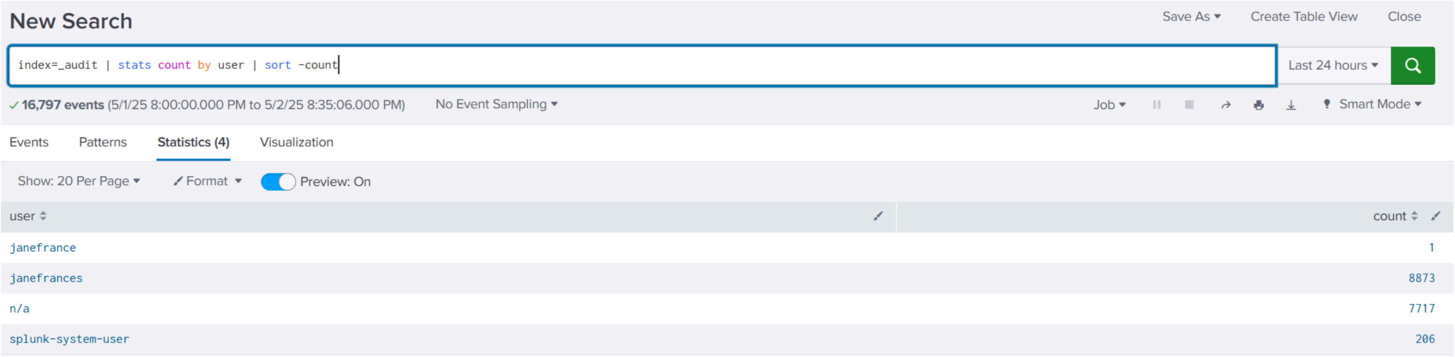


```
index=main OR index=_audit OR index=_internal
(EventCode=4624)
| table _time host Account_Name Source_Network_Address Destination_Network_Address Logon_Type Logon_Process Authentication_Package_Name
| sort - _time
```

✓ 4 events (5/1/25 8:00:00.000 PM to 5/2/25 8:13:13.000 PM)

_time	host	Account_Name	Source_Network_Address	Destination_Network_Address	Logon_Type	Logon_Process	Authentication_Package_Name
2025-05-02 20:09:53.108	CYPRIAN-HOME						
2025-05-02 20:09:53.089	CYPRIAN-HOME						
2025-05-02 20:09:44.882	CYPRIAN-HOME						
2025-05-02 20:09:24.488	CYPRIAN-HOME						

Step 2: Created a search for user logins and sorted and counted by username

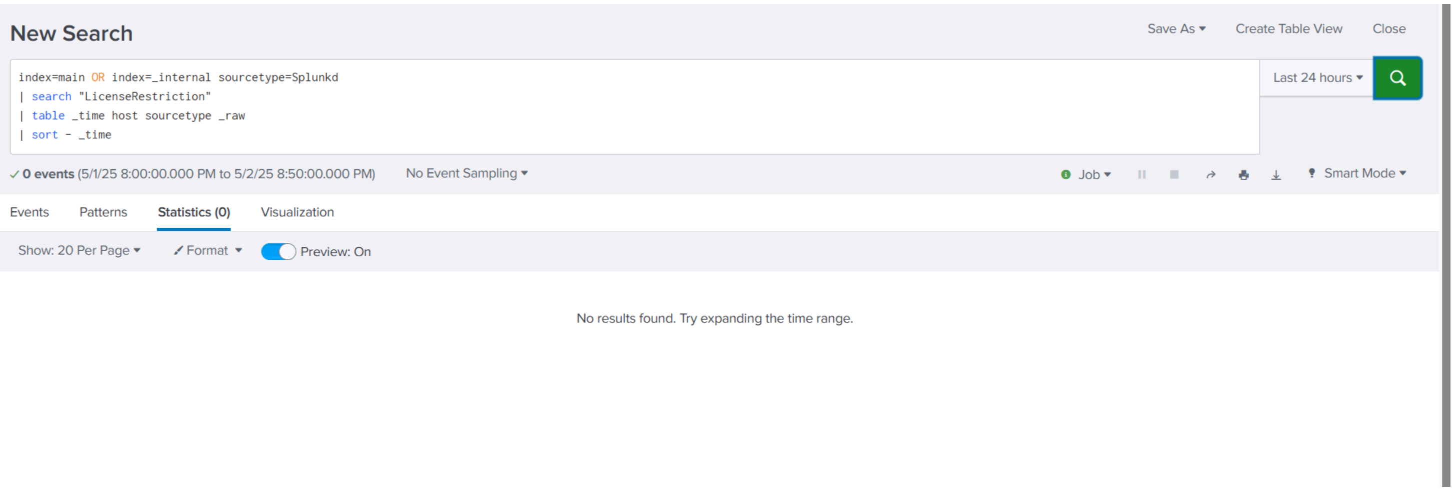


```
index=_audit | stats count by user | sort -count
```

✓ 16,797 events (5/1/25 8:00:00.000 PM to 5/2/25 8:35:06.000 PM)

user	count
janefrance	1
janefrances	8873
n/a	7717
splunk-system-user	206

Step 3: Wrote the SPL for detecting license restriction errors

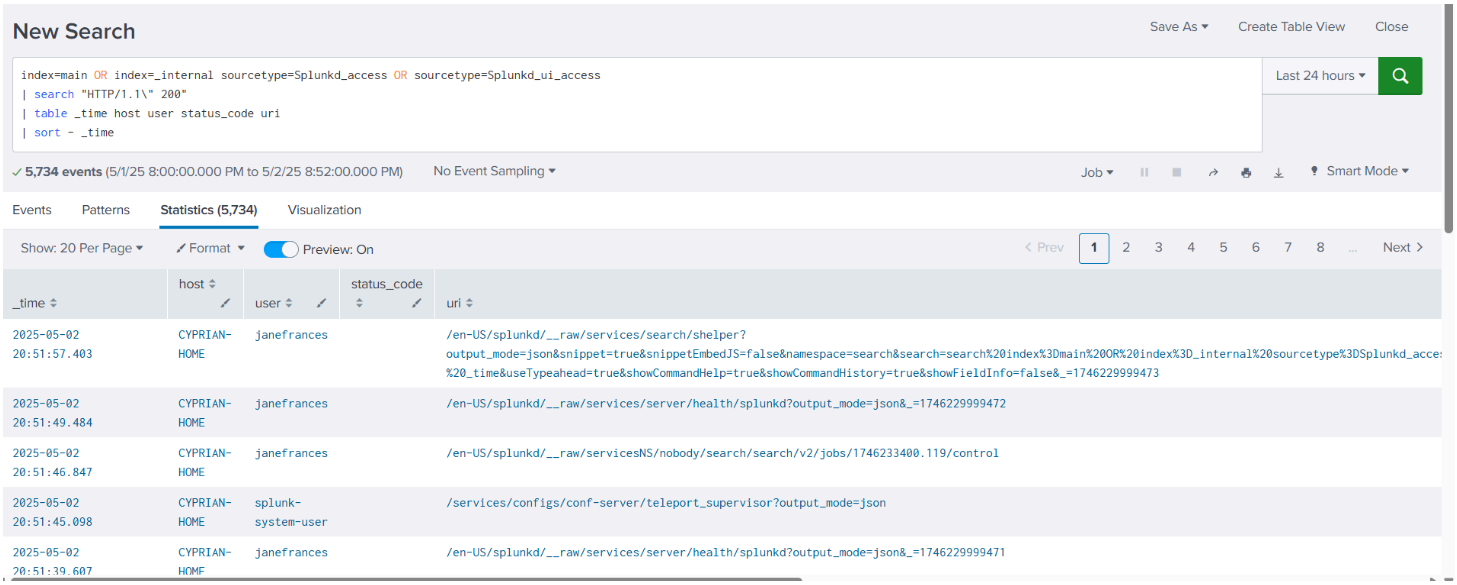


```
index=main OR index=_internal sourcetype=Splunkd
| search "LicenseRestriction"
| table _time host sourcetype _raw
| sort - _time
```

✓ 0 events (5/1/25 8:00:00.000 PM to 5/2/25 8:50:00.000 PM) No Event Sampling ▾

No results found. Try expanding the time range.

Step 4: Wrote the SPL for finding HTTP 202 and 404

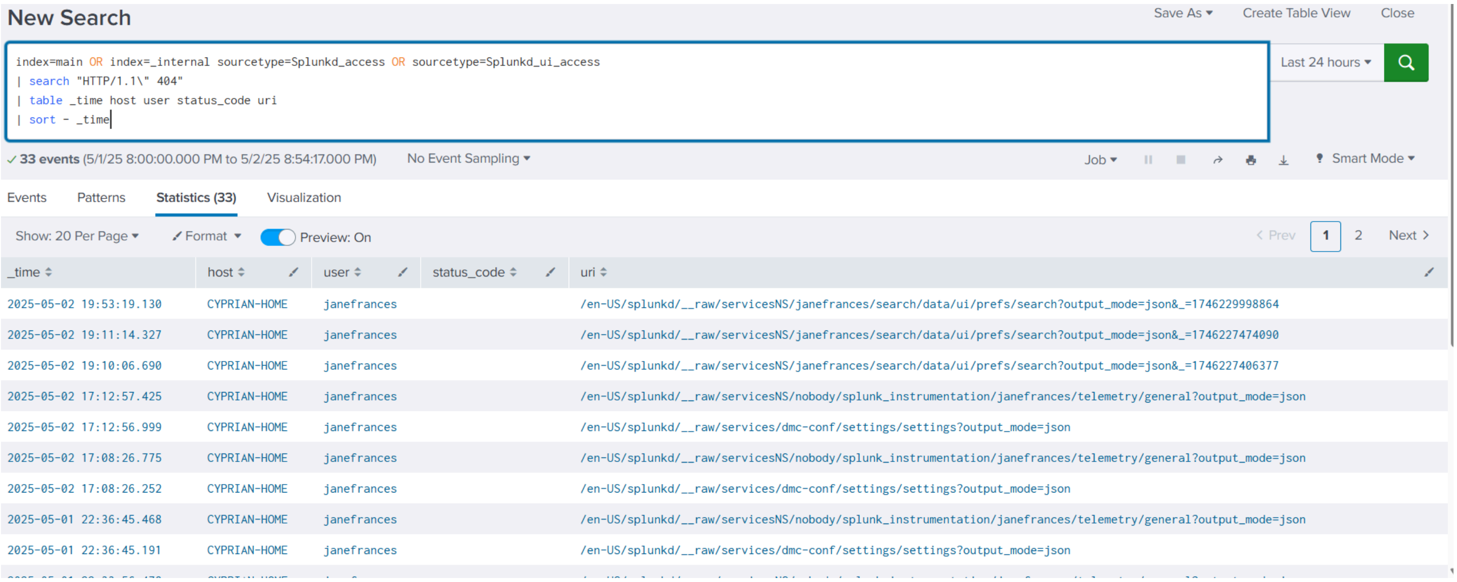


```
index=main OR index=_internal sourcetype=Splunkd_access OR sourcetype=Splunkd_ui_access
| search "HTTP/1.1\" 200"
| table _time host user status_code uri
| sort - _time
```

✓ 5,734 events (5/1/25 8:00:00.000 PM to 5/2/25 8:52:00.000 PM) No Event Sampling ▾

_time	host	user	status_code	uri
2025-05-02 20:51:57.403	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search%20index%3Dmain%20OR%20index%3D_internal%20sourcetype%3DSplunkd_acce %20_time&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1746229999473
2025-05-02 20:51:49.484	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/server/health/splunkd?output_mode=json&_=1746229999472
2025-05-02 20:51:46.847	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/nobody/search/search/v2/jobs/1746233400.119/control
2025-05-02 20:51:45.098	CYPRIAN-HOME	splunk-system-user		/services/configs/conf-server/teleport_supervisor?output_mode=json
2025-05-02 20:51:39.607	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/server/health/splunkd?output_mode=json&_=1746229999471

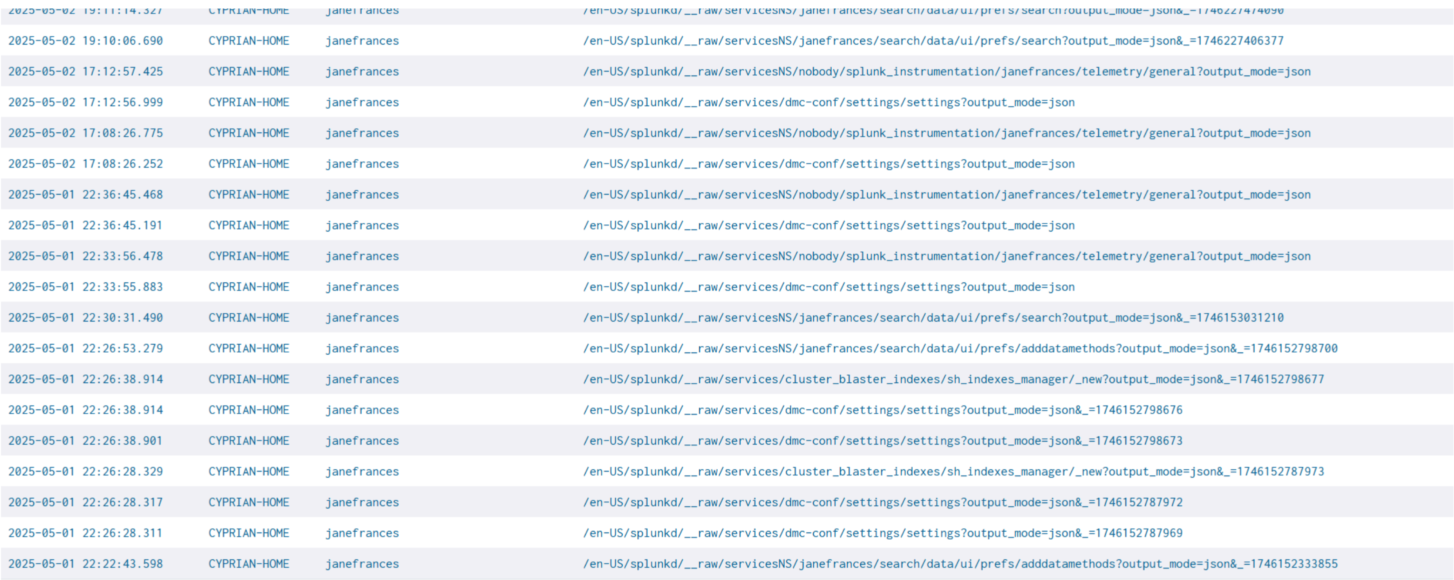
4.2 Searched the below query in the search box to troubleshoot web server or Splunk UI issues by analyzing patterns of 404 errors:



```
index=main OR index=_internal sourcetype=Splunkd_access OR sourcetype=Splunkd_ui_access
| search "HTTP/1.1\" 404"
| table _time host user status_code uri
| sort - _time
```

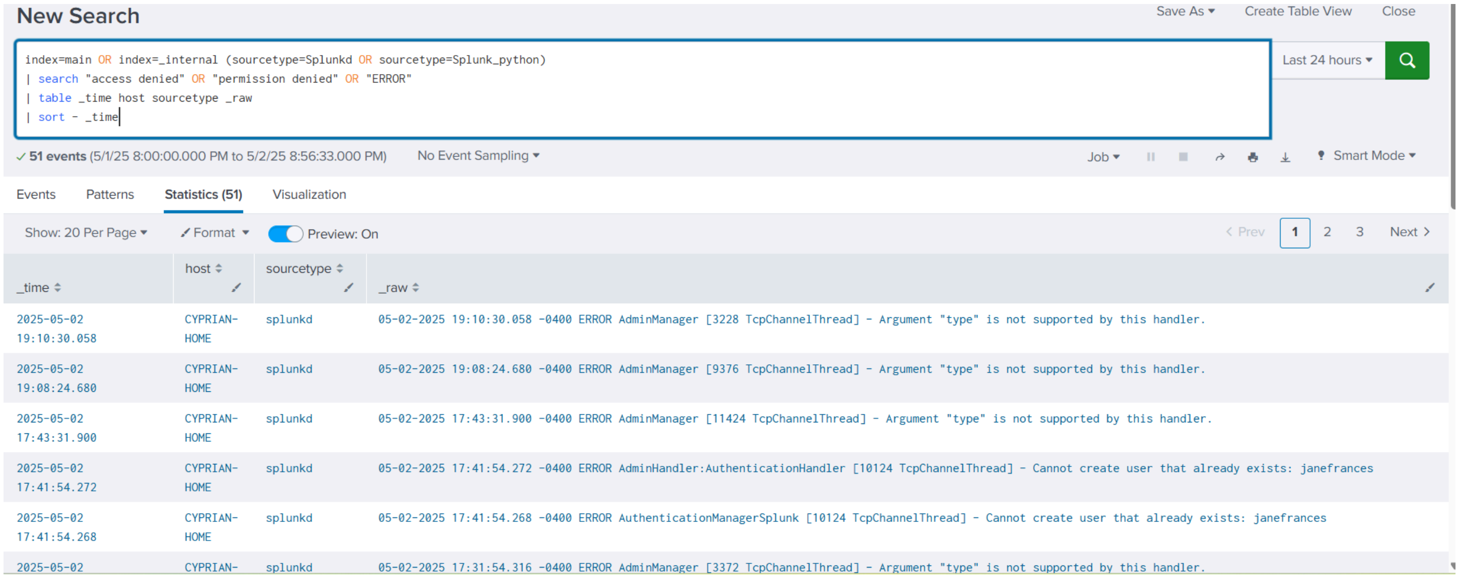
✓ 33 events (5/1/25 8:00:00.000 PM to 5/2/25 8:54:17.000 PM)   No Event Sampling ▾

_time	host	user	status_code	uri
2025-05-02 19:53:19.130	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/janefrances/search/data/ui/prefs/search?output_mode=json&_=1746229998864
2025-05-02 19:11:14.327	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/janefrances/search/data/ui/prefs/search?output_mode=json&_=1746227474090
2025-05-02 19:10:06.690	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/janefrances/search/data/ui/prefs/search?output_mode=json&_=1746227406377
2025-05-02 17:12:57.425	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/nobody/splunk_instrumentation/janefrances/telemetry/general?output_mode=json
2025-05-02 17:12:56.999	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json
2025-05-02 17:08:26.775	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/nobody/splunk_instrumentation/janefrances/telemetry/general?output_mode=json
2025-05-02 17:08:26.252	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json
2025-05-01 22:36:45.468	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/nobody/splunk_instrumentation/janefrances/telemetry/general?output_mode=json
2025-05-01 22:36:45.191	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json



2025-05-02 19:11:14.327	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/janefrances/search/data/ui/prefs/search?output_mode=json&_=1746227474090
2025-05-02 19:10:06.690	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/janefrances/search/data/ui/prefs/search?output_mode=json&_=1746227406377
2025-05-02 17:12:57.425	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/nobody/splunk_instrumentation/janefrances/telemetry/general?output_mode=json
2025-05-02 17:12:56.999	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json
2025-05-02 17:08:26.775	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/nobody/splunk_instrumentation/janefrances/telemetry/general?output_mode=json
2025-05-02 17:08:26.252	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json
2025-05-01 22:36:45.468	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/nobody/splunk_instrumentation/janefrances/telemetry/general?output_mode=json
2025-05-01 22:36:45.191	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json
2025-05-01 22:33:56.478	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/nobody/splunk_instrumentation/janefrances/telemetry/general?output_mode=json
2025-05-01 22:33:55.883	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json
2025-05-01 22:30:31.490	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/janefrances/search/data/ui/prefs/search?output_mode=json&_=1746153031210
2025-05-01 22:26:53.279	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/janefrances/search/data/ui/prefs/adddatamethods?output_mode=json&_=1746152798700
2025-05-01 22:26:38.914	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/cluster_blaster_indexes/sh_indexes_manager/_new?output_mode=json&_=1746152798677
2025-05-01 22:26:38.914	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json&_=1746152798676
2025-05-01 22:26:38.901	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json&_=1746152798673
2025-05-01 22:26:28.329	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/cluster_blaster_indexes/sh_indexes_manager/_new?output_mode=json&_=1746152787973
2025-05-01 22:26:28.317	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json&_=1746152787972
2025-05-01 22:26:28.311	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/services/dmc-conf/settings/settings?output_mode=json&_=1746152787969
2025-05-01 22:22:43.598	CYPRIAN-HOME	janefrances		/en-US/splunkd/__raw/servicesNS/janefrances/search/data/ui/prefs/adddatamethods?output_mode=json&_=1746152333855

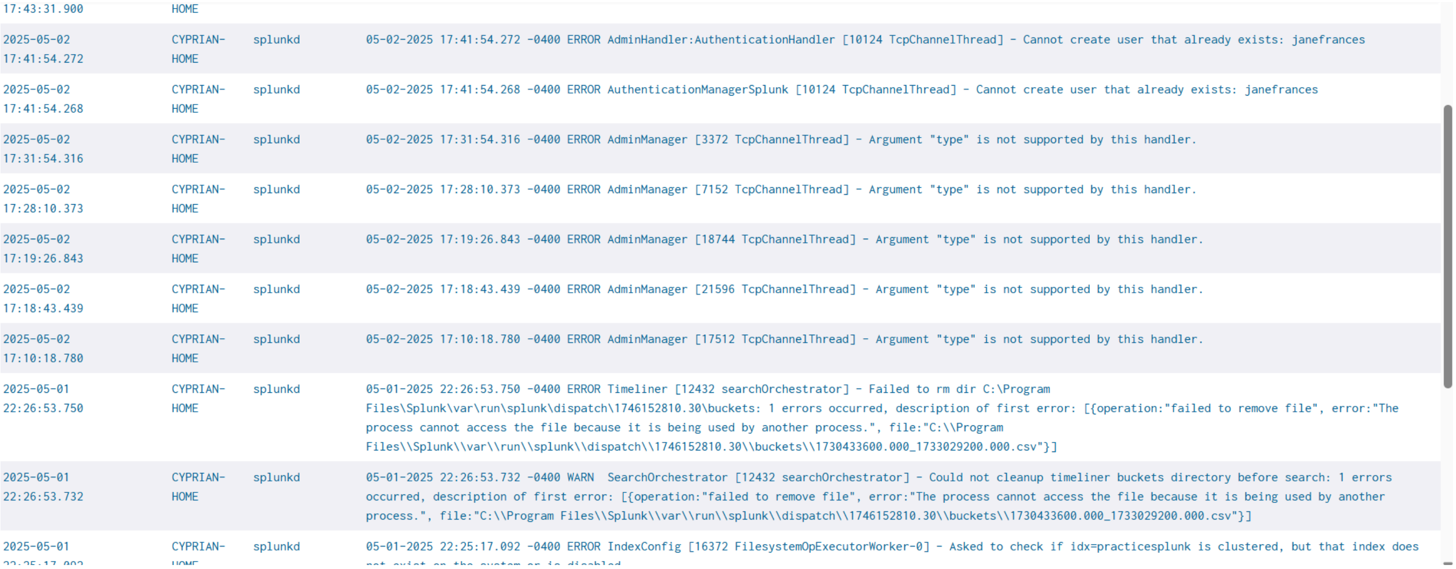
Step 5: Wrote SPL for detecting other errors



```
index=main OR index=_internal (sourcetype=Splunkd OR sourcetype=Splunk_python)
| search "access denied" OR "permission denied" OR "ERROR"
| table _time host sourcetype _raw
| sort - _time
```

✓ 51 events (5/1/25 8:00:00.000 PM to 5/2/25 8:56:33.000 PM) No Event Sampling ▾

_time	host	sourcetype	_raw
2025-05-02 19:10:30.058	CYPRIAN-HOME	splunkd	05-02-2025 19:10:30.058 -0400 ERROR AdminManager [3228 TcpChannelThread] - Argument "type" is not supported by this handler.
2025-05-02 19:08:24.680	CYPRIAN-HOME	splunkd	05-02-2025 19:08:24.680 -0400 ERROR AdminManager [9376 TcpChannelThread] - Argument "type" is not supported by this handler.
2025-05-02 17:43:31.900	CYPRIAN-HOME	splunkd	05-02-2025 17:43:31.900 -0400 ERROR AdminManager [11424 TcpChannelThread] - Argument "type" is not supported by this handler.
2025-05-02 17:41:54.272	CYPRIAN-HOME	splunkd	05-02-2025 17:41:54.272 -0400 ERROR AdminHandler:AuthenticationHandler [10124 TcpChannelThread] - Cannot create user that already exists: janefrances
2025-05-02 17:41:54.268	CYPRIAN-HOME	splunkd	05-02-2025 17:41:54.268 -0400 ERROR AuthenticationManagerSplunk [10124 TcpChannelThread] - Cannot create user that already exists: janefrances
2025-05-02	CYPRIAN-	splunkd	05-02-2025 17:31:54.316 -0400 ERROR AdminManager [3372 TcpChannelThread] - Argument "type" is not supported by this handler.



17:43:31.900	HOME		
2025-05-02 17:41:54.272	CYPRIAN-HOME	splunkd	05-02-2025 17:41:54.272 -0400 ERROR AdminHandler:AuthenticationHandler [10124 TcpChannelThread] - Cannot create user that already exists: janefrances
2025-05-02 17:41:54.268	CYPRIAN-HOME	splunkd	05-02-2025 17:41:54.268 -0400 ERROR AuthenticationManagerSplunk [10124 TcpChannelThread] - Cannot create user that already exists: janefrances
2025-05-02 17:31:54.316	CYPRIAN-HOME	splunkd	05-02-2025 17:31:54.316 -0400 ERROR AdminManager [3372 TcpChannelThread] - Argument "type" is not supported by this handler.
2025-05-02 17:28:10.373	CYPRIAN-HOME	splunkd	05-02-2025 17:28:10.373 -0400 ERROR AdminManager [7152 TcpChannelThread] - Argument "type" is not supported by this handler.
2025-05-02 17:19:26.843	CYPRIAN-HOME	splunkd	05-02-2025 17:19:26.843 -0400 ERROR AdminManager [18744 TcpChannelThread] - Argument "type" is not supported by this handler.
2025-05-02 17:18:43.439	CYPRIAN-HOME	splunkd	05-02-2025 17:18:43.439 -0400 ERROR AdminManager [21596 TcpChannelThread] - Argument "type" is not supported by this handler.
2025-05-02 17:10:18.780	CYPRIAN-HOME	splunkd	05-02-2025 17:10:18.780 -0400 ERROR AdminManager [17512 TcpChannelThread] - Argument "type" is not supported by this handler.
2025-05-01 22:26:53.750	CYPRIAN-HOME	splunkd	05-01-2025 22:26:53.750 -0400 ERROR Timeliner [12432 searchOrchestrator] - Failed to rm dir C:\Program Files\Splunk\var\run\splunk\dispatch\1746152810.30\buckets: 1 errors occurred, description of first error: [{operation:"failed to remove file", error:"The process cannot access the file because it is being used by another process.", file:"C:\\Program Files\\Splunk\\var\\run\\splunk\\dispatch\\1746152810.30\\buckets\\1730433600.000_1733029200.000.csv"}]
2025-05-01 22:26:53.732	CYPRIAN-HOME	splunkd	05-01-2025 22:26:53.732 -0400 WARN SearchOrchestrator [12432 searchOrchestrator] - Could not cleanup timeliner buckets directory before search: 1 errors occurred, description of first error: [{operation:"failed to remove file", error:"The process cannot access the file because it is being used by another process.", file:"C:\\Program Files\\Splunk\\var\\run\\splunk\\dispatch\\1746152810.30\\buckets\\1730433600.000_1733029200.000.csv"}]
2025-05-01 22:25:17.092	CYPRIAN-HOME	splunkd	05-01-2025 22:25:17.092 -0400 ERROR IndexConfig [16372 FilesystemOpExecutorWorker-0] - Asked to check if idx=practicesplunk is clustered, but that index does not exist on the system or is disabled