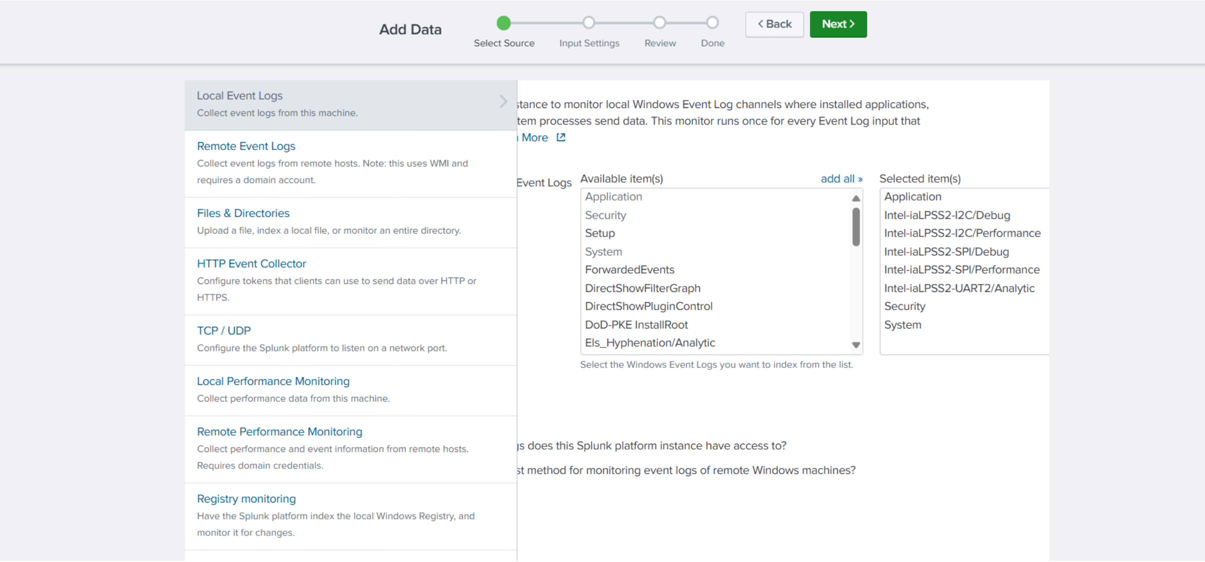
Local Host Log Upload

Select the log type you want displayed. I’m interested in exploring usual system, security, application and Windows logs.



Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Registry monitoring
Have the Splunk platform index the local Windows Registry, and monitor it for changes.

stance to monitor local Windows Event Log channels where installed applications,
tem processes send data. This monitor runs once for every Event Log input that
More

Event Logs

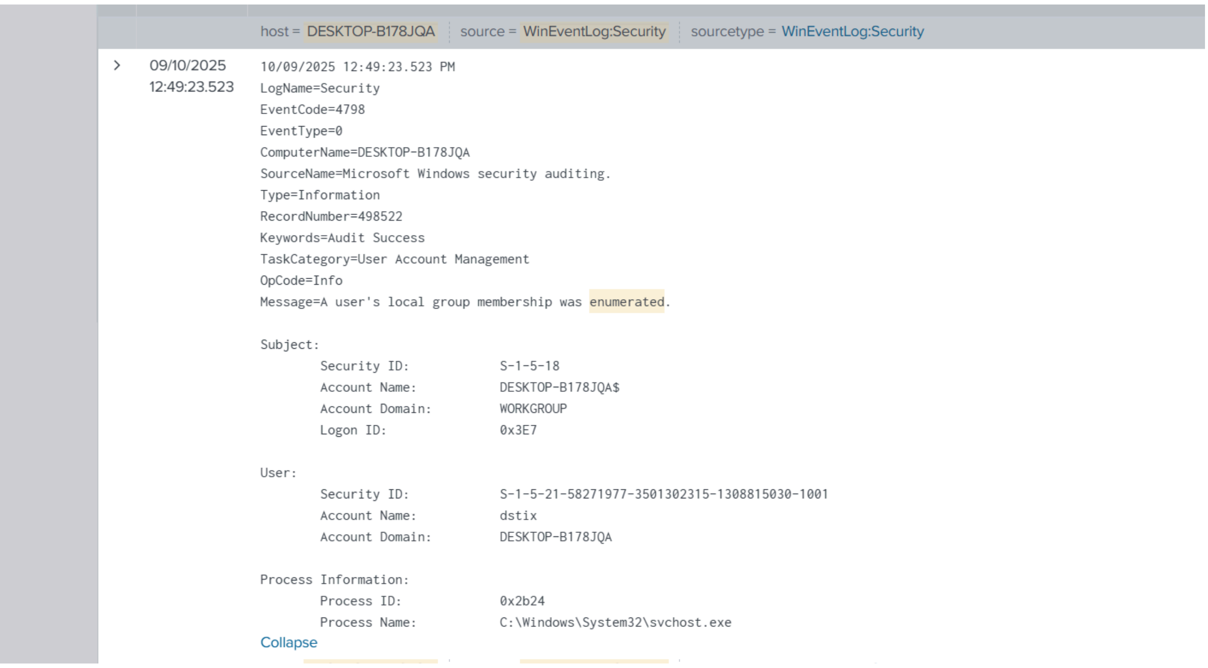
Available item(s) add all »	Selected item(s)
Application	Application
Security	Intel-iaLPSS2-I2C/Debug
Setup	Intel-iaLPSS2-I2C/Performance
System	Intel-iaLPSS2-SPI/Debug
ForwardedEvents	Intel-iaLPSS2-SPI/Performance
DirectShowFilterGraph	Intel-iaLPSS2-UART2/Analytic
DirectShowPluginControl	Security
DoD-PKE InstallRoot	System
Els_Hyphenation/Analytic	

Select the Windows Event Logs you want to index from the list.

s does this Splunk platform instance have access to?

st method for monitoring event logs of remote Windows machines?

Investigate logs, what does each attribute represent. Processes created and their respective child processes.



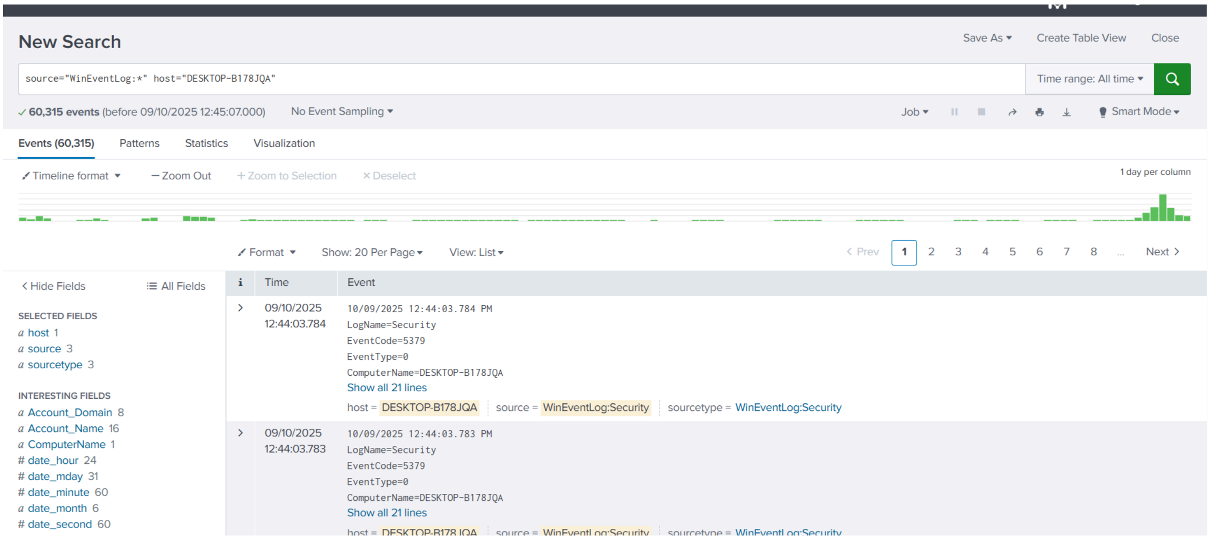
host = DESKTOP-B178JQA | source = WinEventLog:Security | sourcetype = WinEventLog:Security

09/10/2025
12:49:23.523

```
10/09/2025 12:49:23.523 PM
LogName=Security
EventCode=4798
EventType=0
ComputerName=DESKTOP-B178JQA
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=498522
Keywords=Audit Success
TaskCategory=User Account Management
OpCode=Info
Message=A user's local group membership was enumerated.

Subject:
        Security ID:            S-1-5-18
        Account Name:           DESKTOP-B178JQA$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

User:
        Security ID:            S-1-5-21-58271977-3501302315-1308815030-1001
        Account Name:           dstix
        Account Domain:         DESKTOP-B178JQA

Process Information:
        Process ID:             0x2b24
        Process Name:           C:\Windows\System32\svchost.exe
```

Collapse

HAPPY SPLUNKIN’



```
source="WinEventLog:*" host="DESKTOP-B178JQA"
```

✓ **60,315 events** (before 09/10/2025 12:45:07.000)

SELECTED FIELDS

- *a* host 1
- *a* source 3
- *a* sourcetype 3

INTERESTING FIELDS

- *a* Account_Domain 8
- *a* Account_Name 16
- *a* ComputerName 1
- # date_hour 24
- # date_mday 31
- # date_minute 60
- *a* date_month 6
- # date_second 60

09/10/2025 12:44:03.784

```
10/09/2025 12:44:03.784 PM
LogName=Security
EventCode=5379
EventType=0
ComputerName=DESKTOP-B178JQA
```

host = DESKTOP-B178JQA | source = WinEventLog:Security | sourcetype = WinEventLog:Security

09/10/2025 12:44:03.783

```
10/09/2025 12:44:03.783 PM
LogName=Security
EventCode=5379
EventType=0
ComputerName=DESKTOP-B178JQA
```

host = DESKTOP-B178JQA | source = WinEventLog:Security | sourcetype = WinEventLog:Security