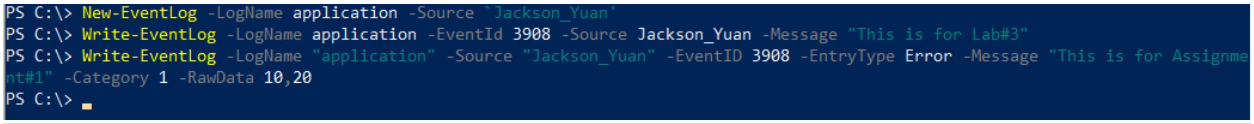
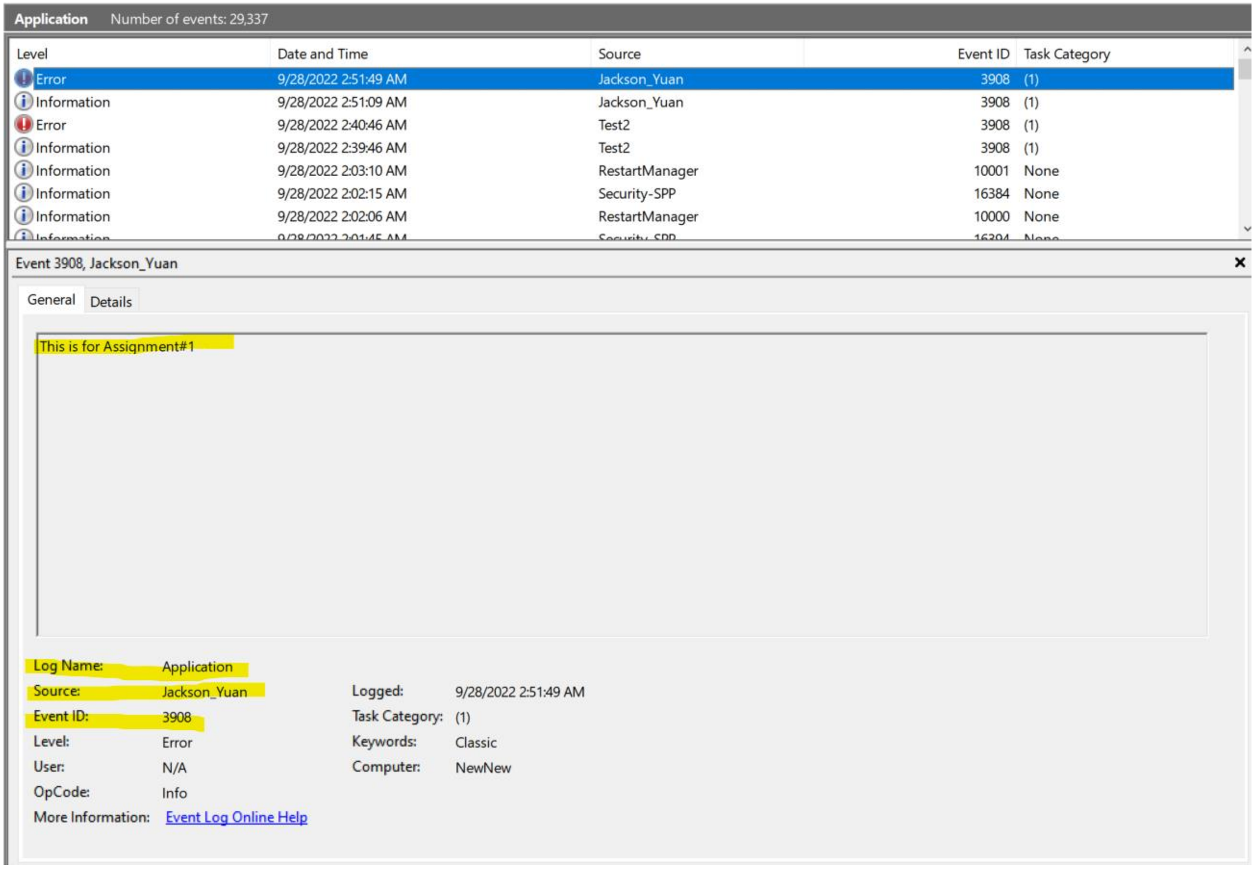
# In-Class Lab 3

1. Create Windows event using PowerShell (**I have used “3908” instead of “1229_3908” as the underscore was unable to convert value "1229_3908" to type "System.Int32".**)



```
PS C:\> New-EventLog -LogName application -Source `Jackson_Yuan'
PS C:\> Write-EventLog -LogName application -EventId 3908 -Source Jackson_Yuan -Message "This is for Lab#3"
PS C:\> Write-EventLog -LogName "application" -Source "Jackson_Yuan" -EventID 3908 -EntryType Error -Message "This is for Assignme
nt#1" -Category 1 -RawData 10,20
PS C:\> _
```



**Application** Number of events: 29,337

| Level | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Error | 9/28/2022 2:51:49 AM | Jackson_Yuan | 3908 | (1) |
| Information | 9/28/2022 2:51:09 AM | Jackson_Yuan | 3908 | (1) |
| Error | 9/28/2022 2:40:46 AM | Test2 | 3908 | (1) |
| Information | 9/28/2022 2:39:46 AM | Test2 | 3908 | (1) |
| Information | 9/28/2022 2:03:10 AM | RestartManager | 10001 | None |
| Information | 9/28/2022 2:02:15 AM | Security-SPP | 16384 | None |
| Information | 9/28/2022 2:02:06 AM | RestartManager | 10000 | None |
| Information | 9/28/2022 2:01:45 AM | Security-SPP | 16384 | None |

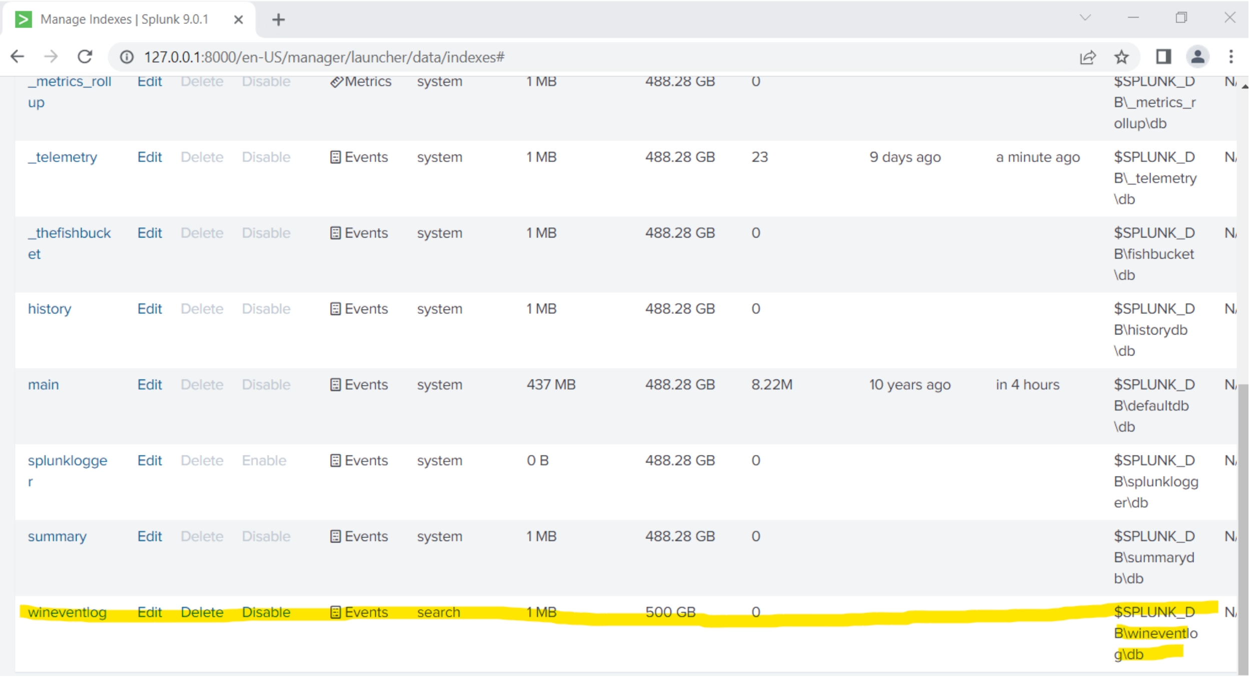
Event 3908, Jackson_Yuan

This is for Assignment#1

Log Name: Application
Source: Jackson_Yuan
Event ID: 3908
Level: Error
User: N/A
OpCode: Info
More Information: Event Log Online Help

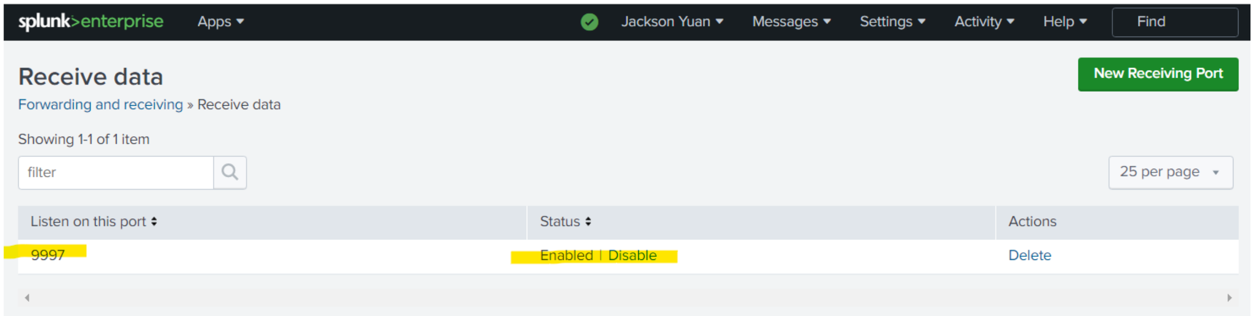
Logged: 9/28/2022 2:51:49 AM
Task Category: (1)
Keywords: Classic
Computer: NewNew

2. Setting up the forwarder index for splunk


Manage Indexes | Splunk 9.0.1
127.0.0.1:8000/en-US/manager/launcher/data/indexes#

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| _metrics_rollup | Edit | Delete | Disable | Metrics | system | 1 MB | 488.28 GB | 0 | | | $SPLUNK_DB_metrics_rollup\db | N |
| _telemetry | Edit | Delete | Disable | Events | system | 1 MB | 488.28 GB | 23 | 9 days ago | a minute ago | $SPLUNK_DB_telemetry\db | N |
| _thefishbucket | Edit | Delete | Disable | Events | system | 1 MB | 488.28 GB | 0 | | | $SPLUNK_DB\fishbucket\db | N |
| history | Edit | Delete | Disable | Events | system | 1 MB | 488.28 GB | 0 | | | $SPLUNK_DB\historydb\db | N |
| main | Edit | Delete | Disable | Events | system | 437 MB | 488.28 GB | 8.22M | 10 years ago | in 4 hours | $SPLUNK_DB\defaultdb\db | N |
| splunklogger | Edit | Delete | Enable | Events | system | 0 B | 488.28 GB | 0 | | | $SPLUNK_DB\splunklogger\db | N |
| summary | Edit | Delete | Disable | Events | system | 1 MB | 488.28 GB | 0 | | | $SPLUNK_DB\summarydb\db | N |
| wineventlog | Edit | Delete | Disable | Events | search | 1 MB | 500 GB | 0 | | | $SPLUNK_DB\wineventlog\db | N |

3. Configure settings for receiving port



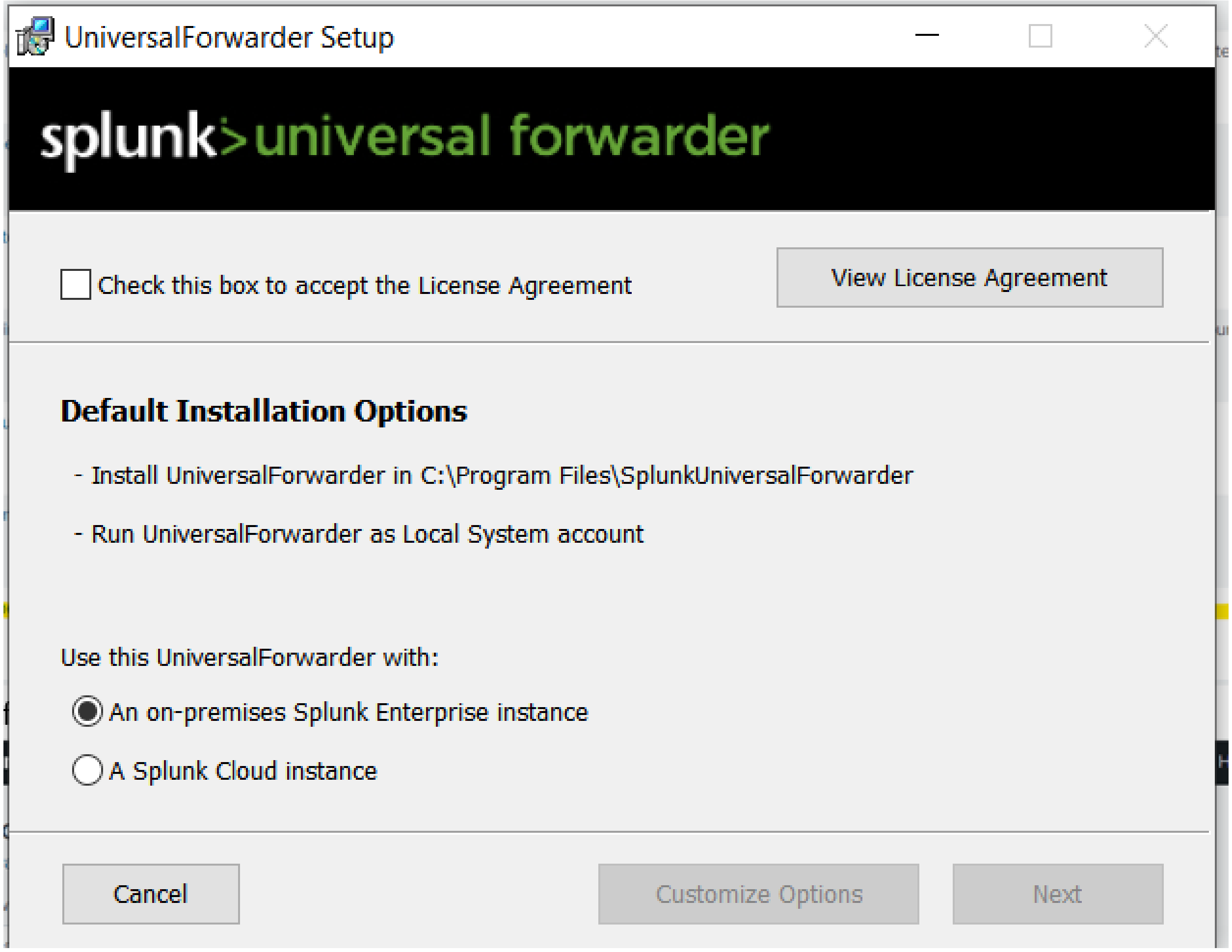
Receive data

Forwarding and receiving » Receive data

Showing 1-1 of 1 item

| Listen on this port | Status | Actions |
|---|---|---|
| 9997 | Enabled \| Disable | Delete |

4. Installing splunk universal forwarder on host machine



□ Check this box to accept the License Agreement

**Default Installation Options**

- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder

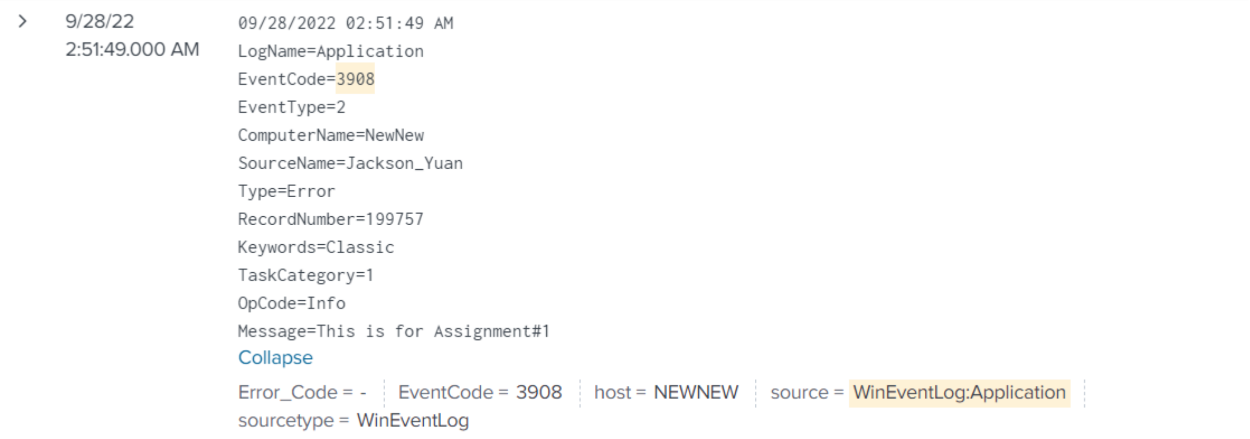
- Run UniversalForwarder as Local System account

Use this UniversalForwarder with:

● An on-premises Splunk Enterprise instance

○ A Splunk Cloud instance

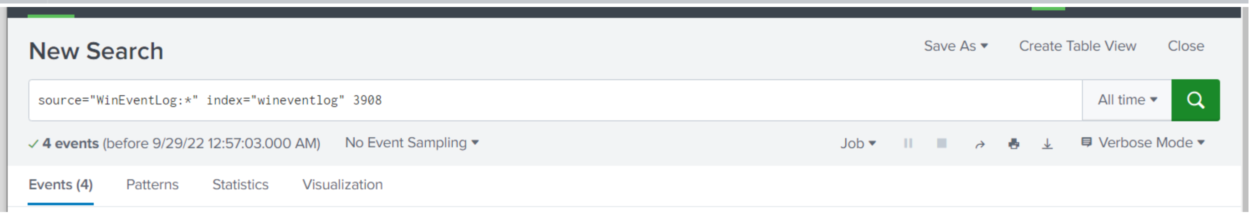
5. Searching for host windows event created in Lab #3



9/28/22
2:51:49.000 AM

```
09/28/2022 02:51:49 AM
LogName=Application
EventCode=3908
EventType=2
ComputerName=NewNew
SourceName=Jackson_Yuan
Type=Error
RecordNumber=199757
Keywords=Classic
TaskCategory=1
OpCode=Info
Message=This is for Assignment#1
```

Error_Code = - | EventCode = 3908 | host = NEWNEW | source = WinEventLog:Application | sourcetype = WinEventLog



New Search

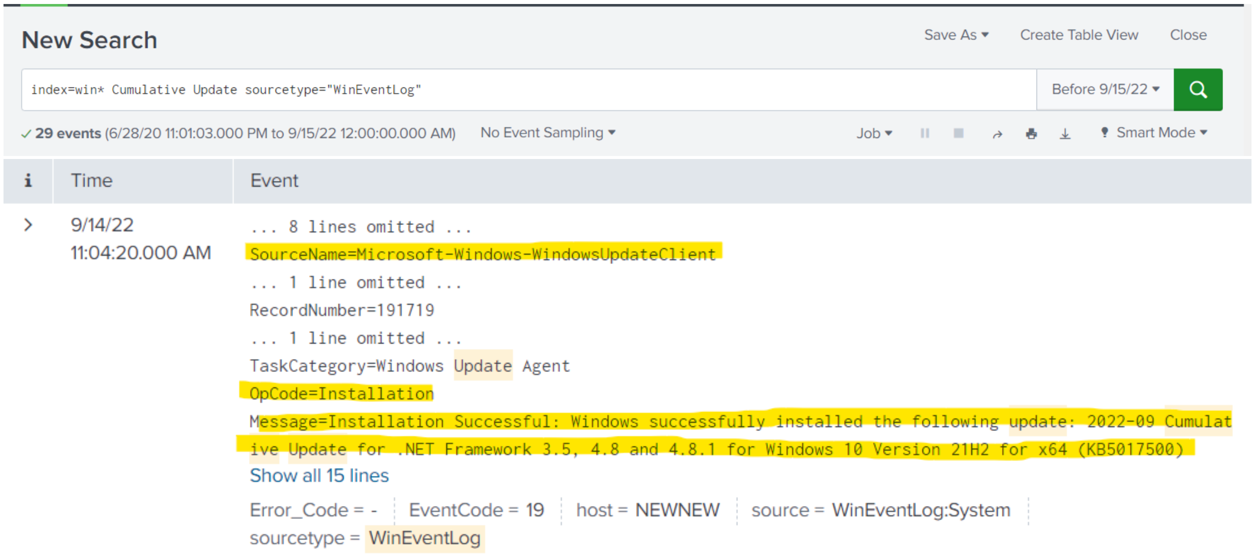
```
source="WinEventLog:*" index="wineventlog" 3908
```

All time ▾

✓ **4 events** (before 9/29/22 12:57:03.000 AM) No Event Sampling ▾

# In-Class Lab 4

1. Search query to forward to Splunk information about installed patches for your second host computer



```
index=win* Cumulative Update sourcetype="WinEventLog"
```

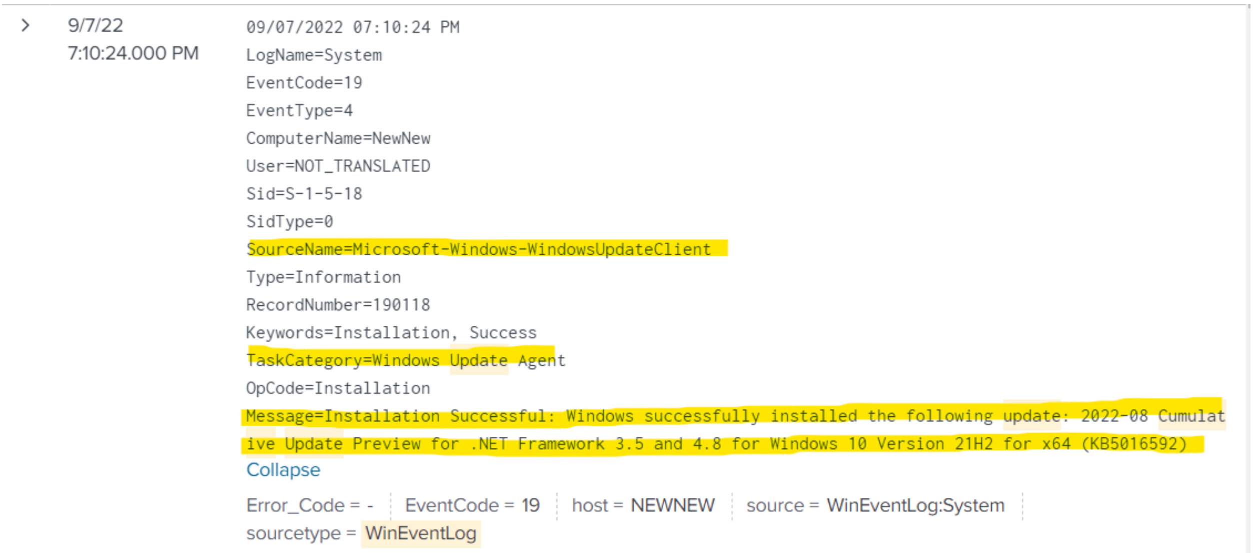
✓ 29 events (6/28/20 11:01:03.000 PM to 9/15/22 12:00:00.000 AM)

9/14/22 11:04:20.000 AM

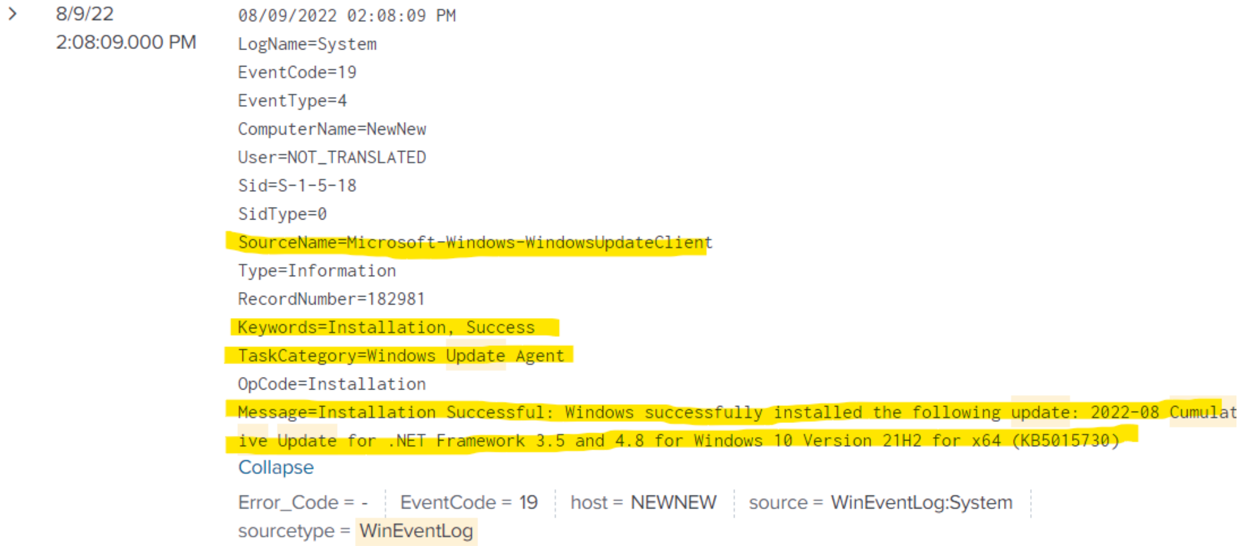
```
... 8 lines omitted ...
SourceName=Microsoft-Windows-WindowsUpdateClient
... 1 line omitted ...
RecordNumber=191719
... 1 line omitted ...
TaskCategory=Windows Update Agent
OpCode=Installation
Message=Installation Successful: Windows successfully installed the following update: 2022-09 Cumulat
ive Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 21H2 for x64 (KB5017500)
```

Show all 15 lines

Error_Code = - | EventCode = 19 | host = NEWNEW | source = WinEventLog:System | sourcetype = WinEventLog

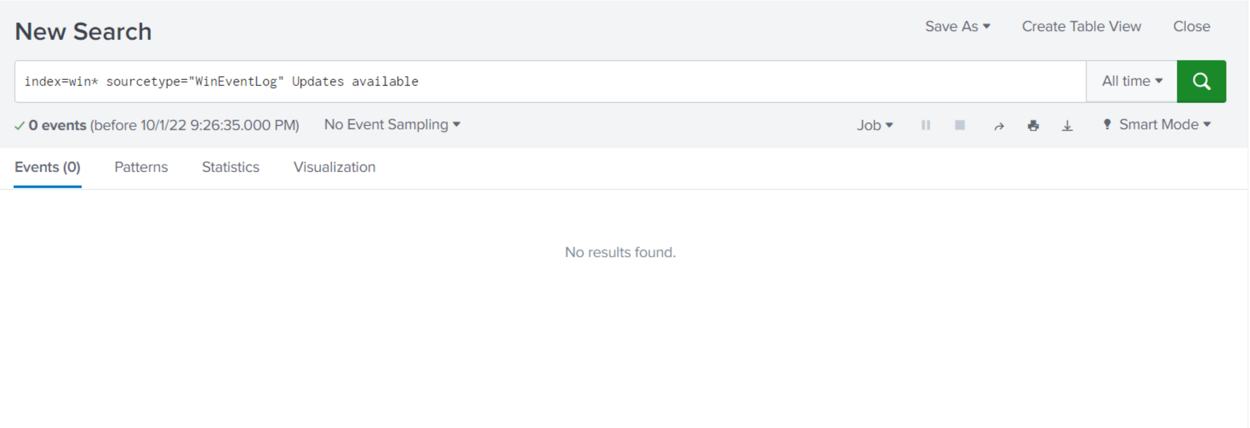


```
> 9/7/22            09/07/2022 07:10:24 PM
  7:10:24.000 PM    LogName=System
                    EventCode=19
                    EventType=4
                    ComputerName=NewNew
                    User=NOT_TRANSLATED
                    Sid=S-1-5-18
                    SidType=0
                    SourceName=Microsoft-Windows-WindowsUpdateClient
                    Type=Information
                    RecordNumber=190118
                    Keywords=Installation, Success
                    TaskCategory=Windows Update Agent
                    OpCode=Installation
                    Message=Installation Successful: Windows successfully installed the following update: 2022-08 Cumulat
                    ive Update Preview for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 for x64 (KB5016592)
                    Collapse
                    Error_Code = -   EventCode = 19   host = NEWNEW   source = WinEventLog:System
                    sourcetype = WinEventLog
```



```
> 8/9/22            08/09/2022 02:08:09 PM
  2:08:09.000 PM    LogName=System
                    EventCode=19
                    EventType=4
                    ComputerName=NewNew
                    User=NOT_TRANSLATED
                    Sid=S-1-5-18
                    SidType=0
                    SourceName=Microsoft-Windows-WindowsUpdateClient
                    Type=Information
                    RecordNumber=182981
                    Keywords=Installation, Success
                    TaskCategory=Windows Update Agent
                    OpCode=Installation
                    Message=Installation Successful: Windows successfully installed the following update: 2022-08 Cumulat
                    ive Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 for x64 (KB5015730)
                    Collapse
                    Error_Code = -   EventCode = 19   host = NEWNEW   source = WinEventLog:System
                    sourcetype = WinEventLog
```

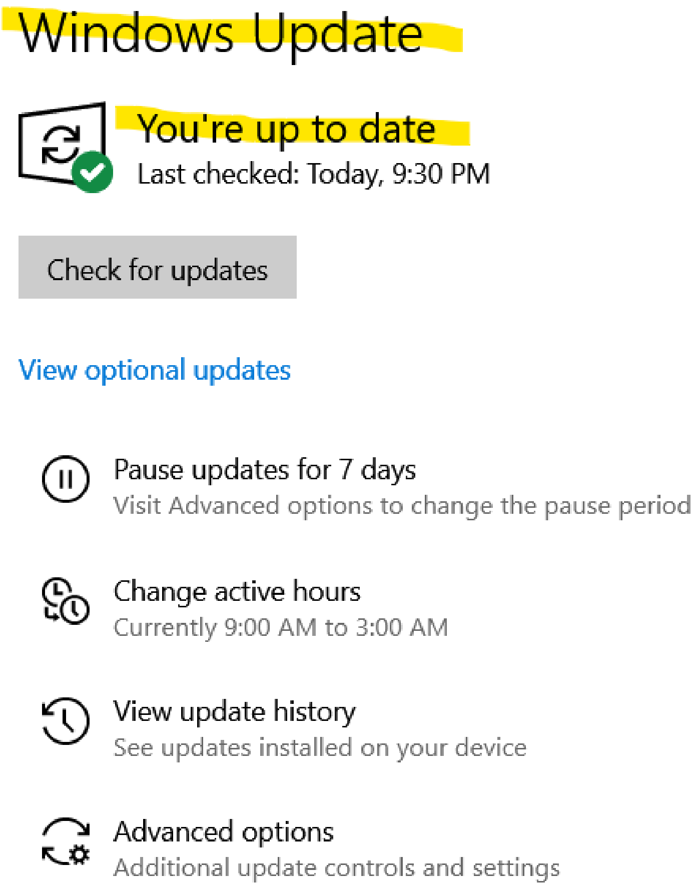
2. Checking for available patches for my host machine. This yielded no results as my host computer is currently up to date with the latest patches.



```
index=win* sourcetype="WinEventLog" Updates available
```

✓ **0 events** (before 10/1/22 9:26:35.000 PM)

No results found.



Windows Update

You're up to date

Last checked: Today, 9:30 PM

Pause updates for 7 days

Visit Advanced options to change the pause period

Change active hours

Currently 9:00 AM to 3:00 AM

View update history

See updates installed on your device

Advanced options

Additional update controls and settings