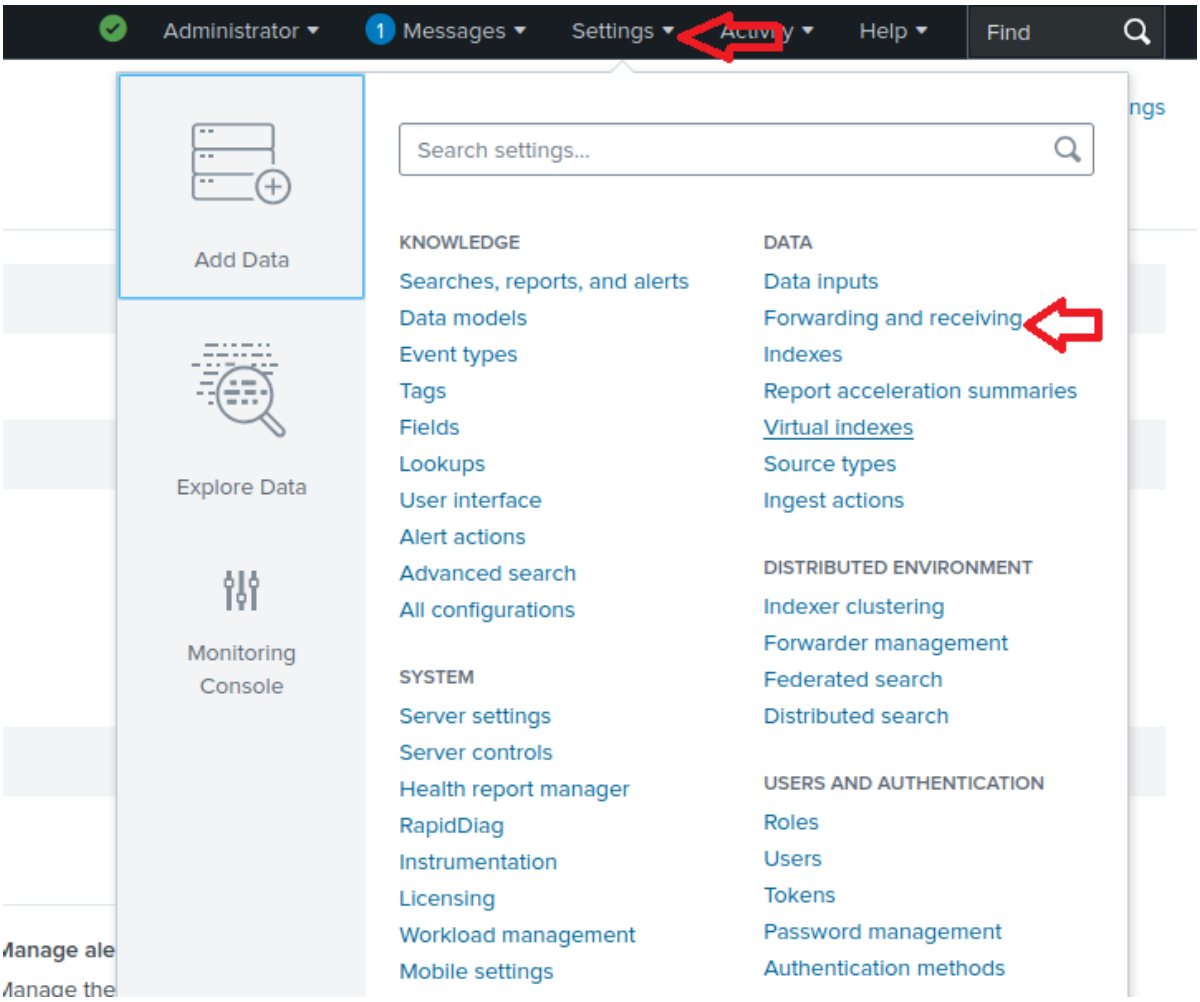
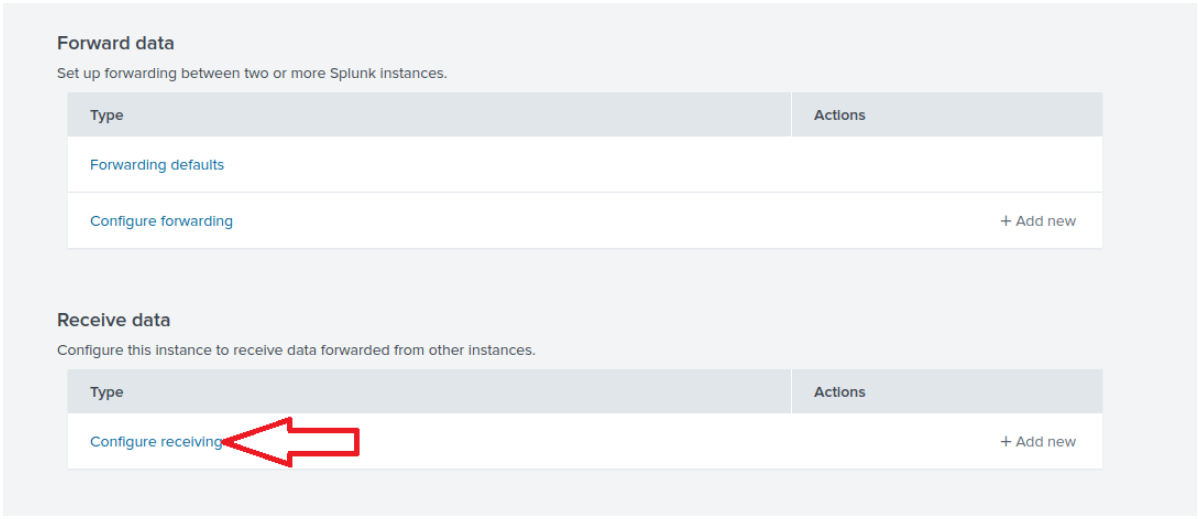
Splunk Server Setup

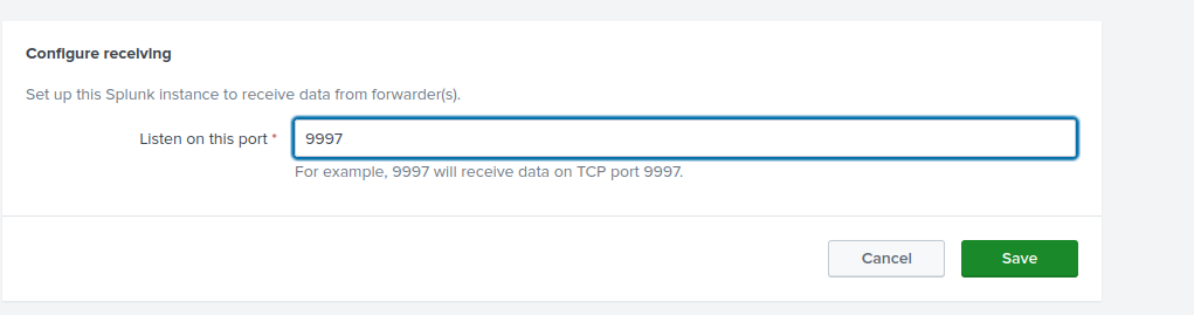
1. Set up **Receiving** on Splunk Server

   Navigate to Settings->Forwarding and receving

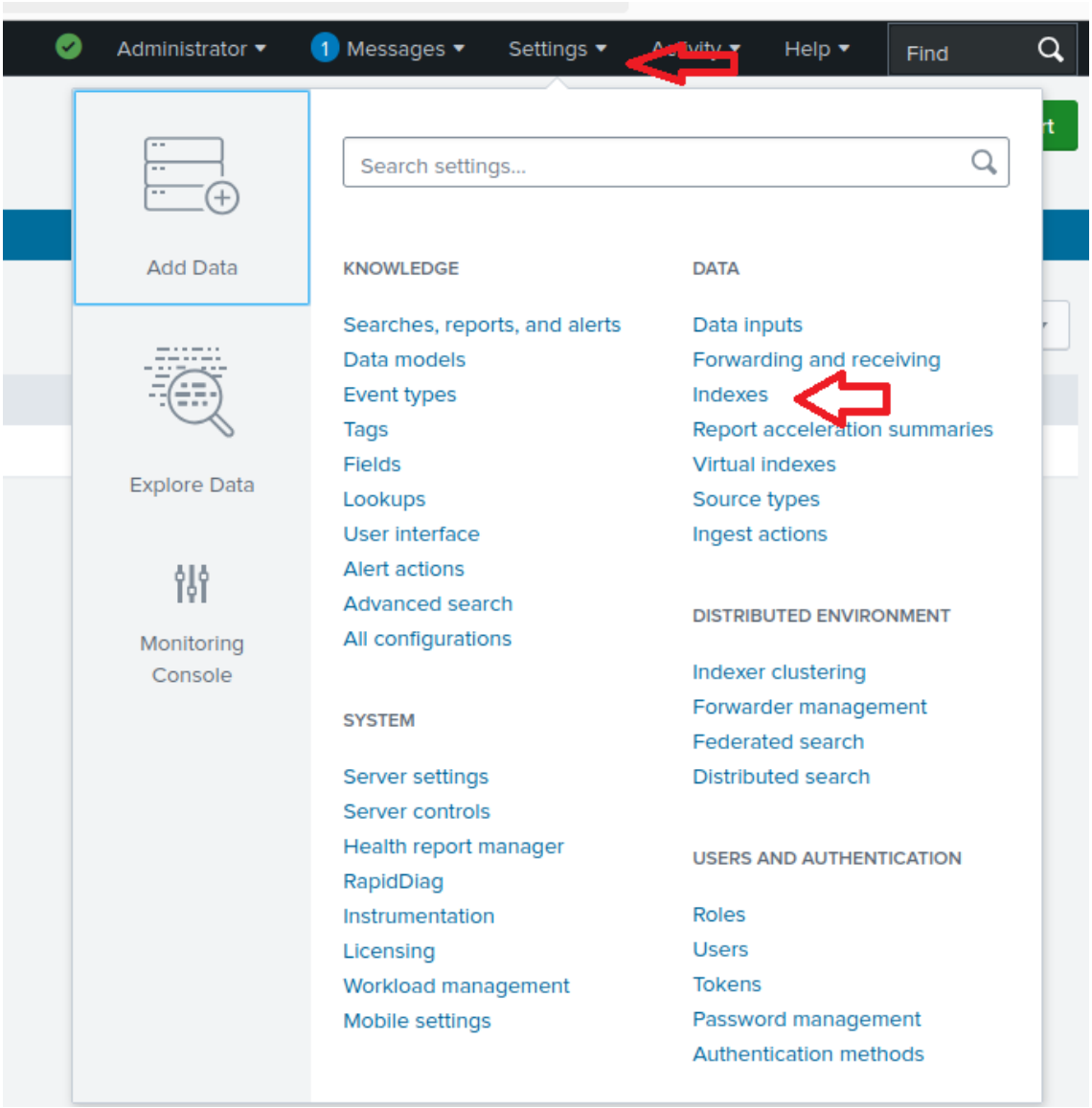




   Click **New Receiving Port**, then enter default port 9997

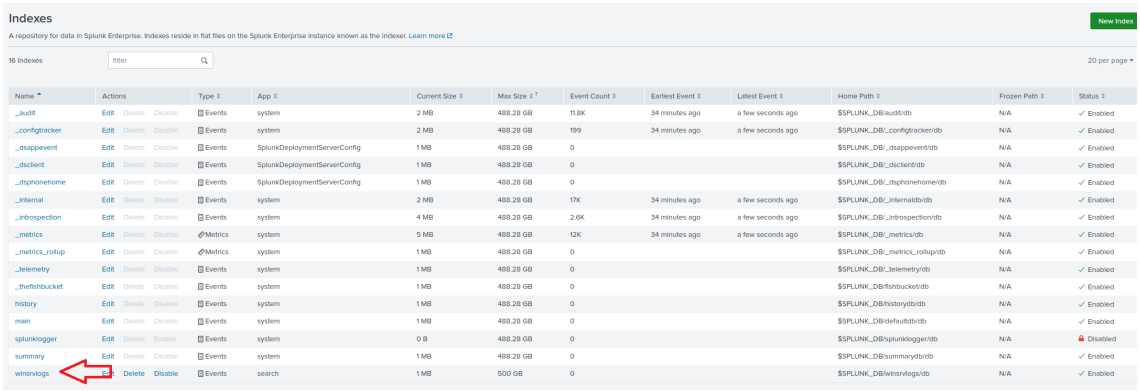


2. Set up **Index** on Splunk server



Click **New Index**

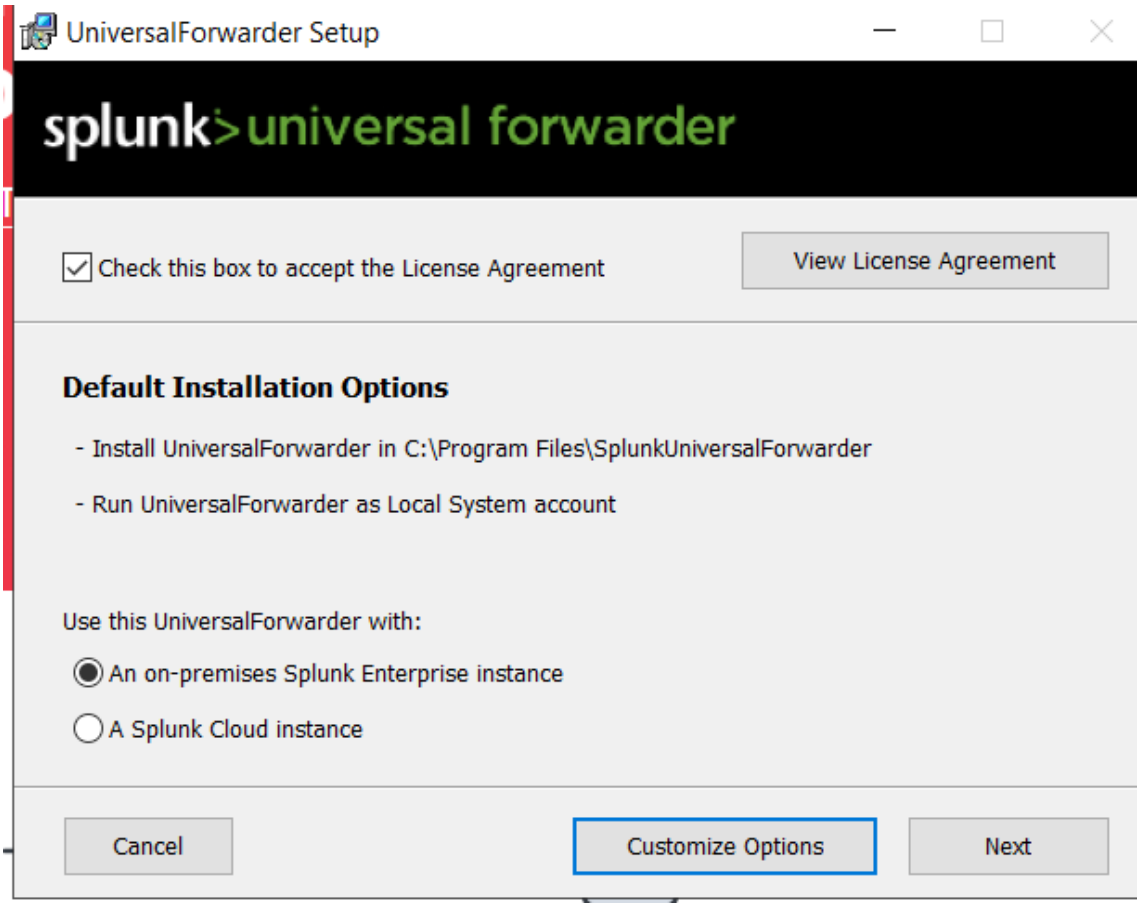
Input **winsrvlogs** as Index Name and **Save**

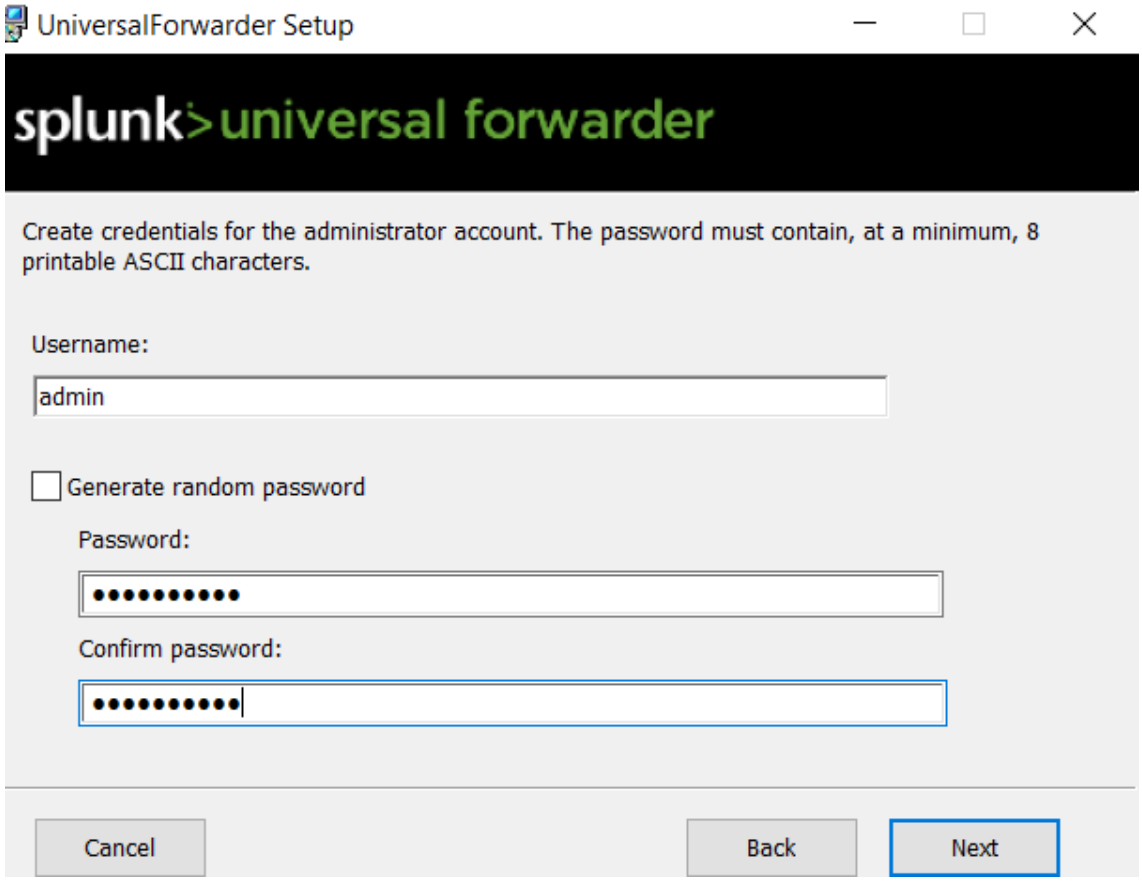


Install Splunk forwarder on Windows Server 2019

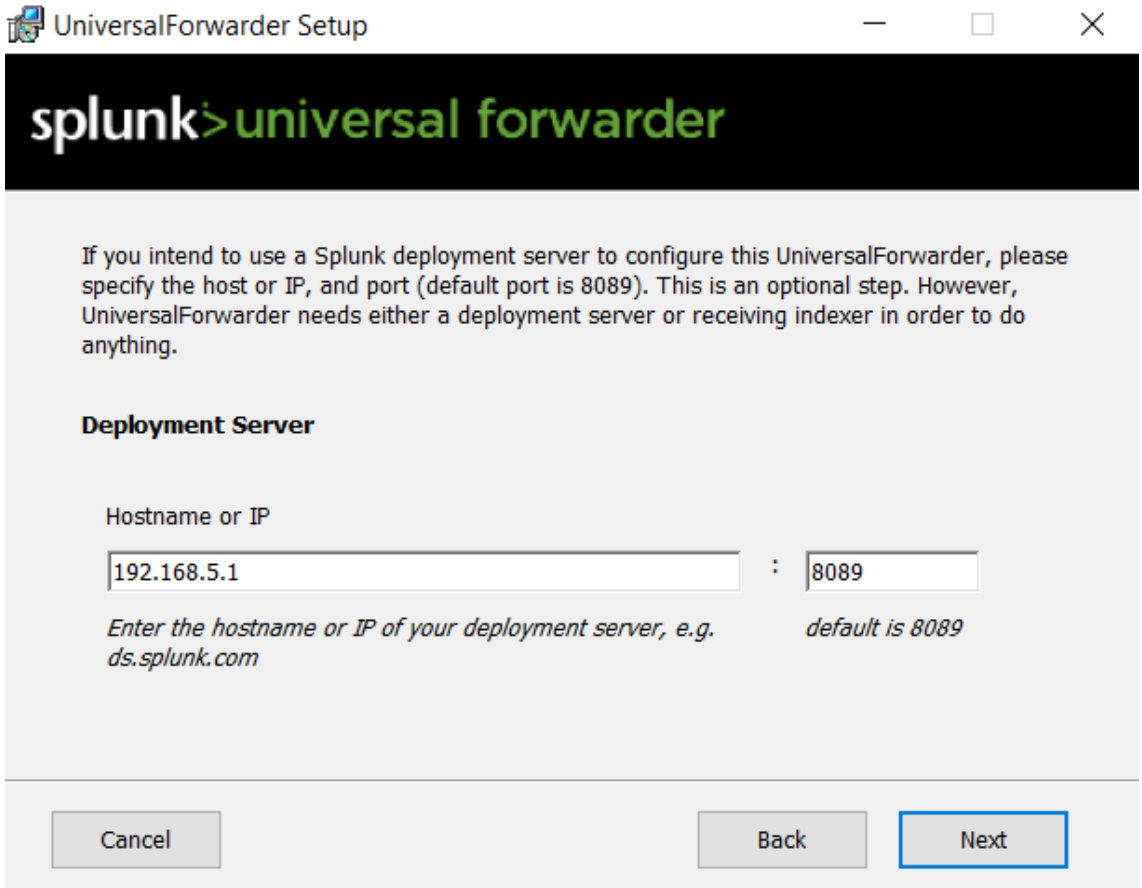
Go to link https://www.splunk.com/en_us/download/universal-forwarder.html to download universal forwarder for Windows server. The purpose of deploying splunk forwarder on windows server is to send logs and everything from Windows Server to Splunk for future investigation.

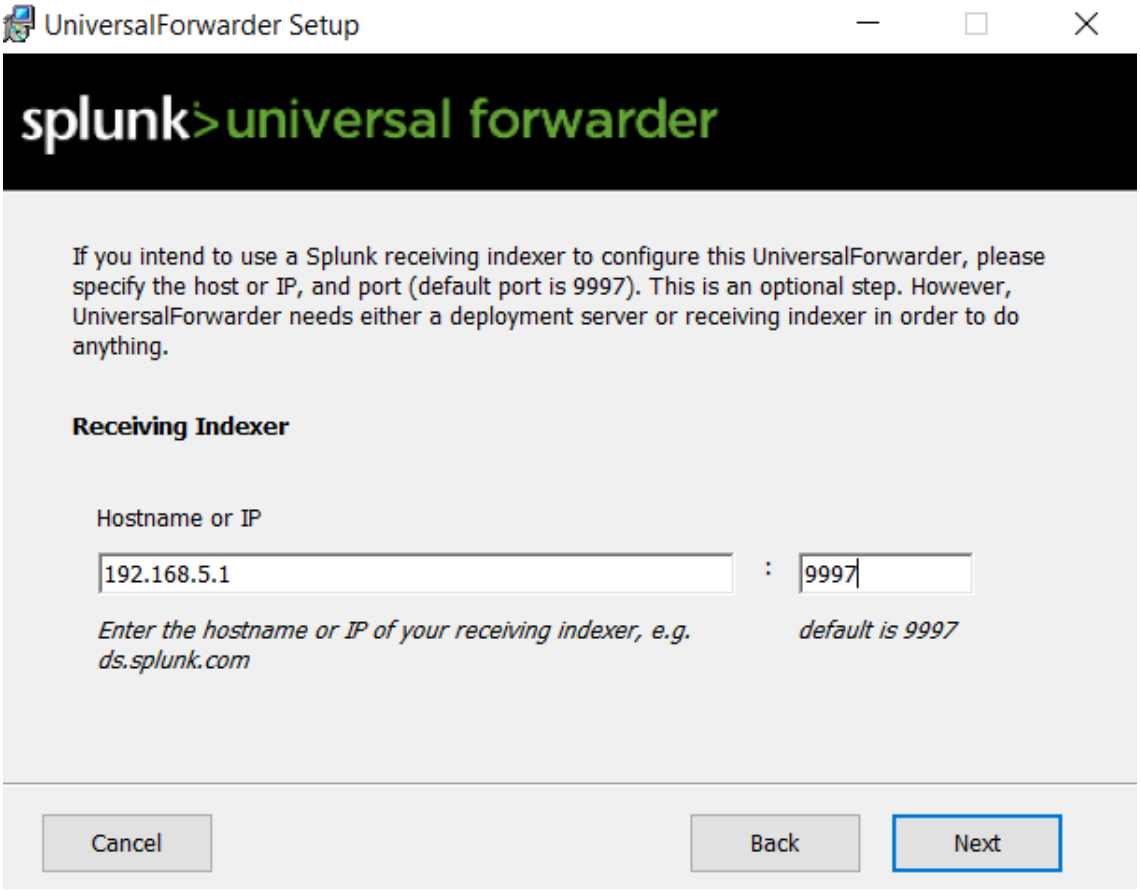
1. Install Splunk forwarder on Windows and just click **Next**





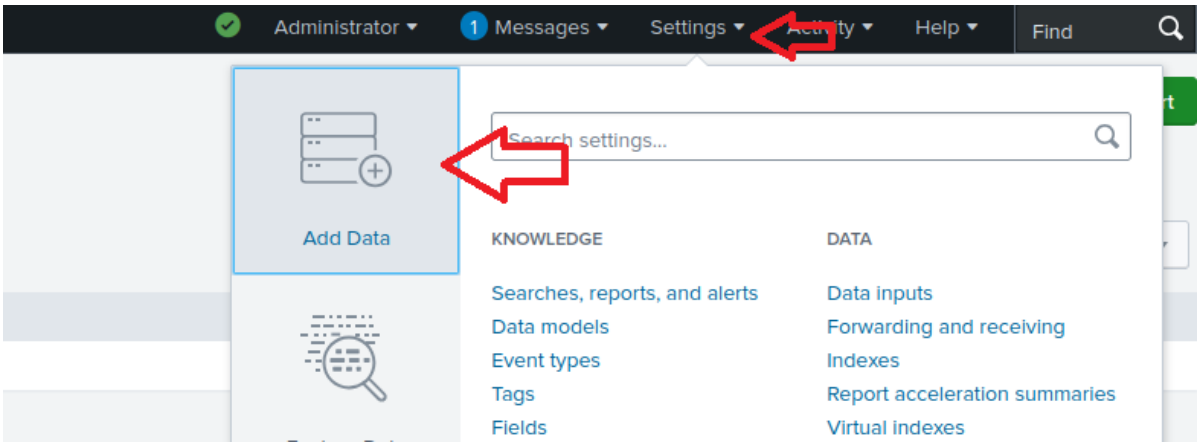
Below is the reason to setup static ip on splunk server.



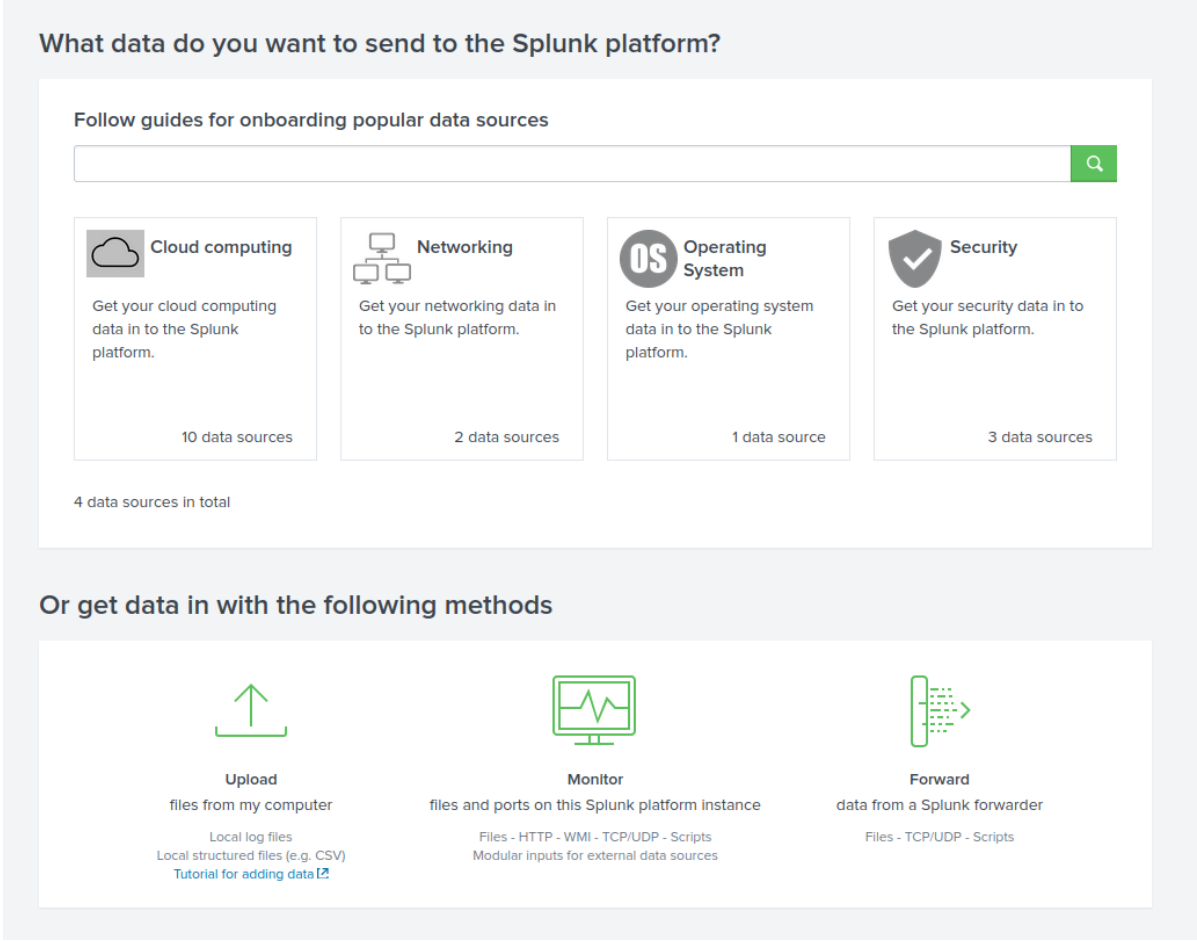


Configure Forward on Splunk Server

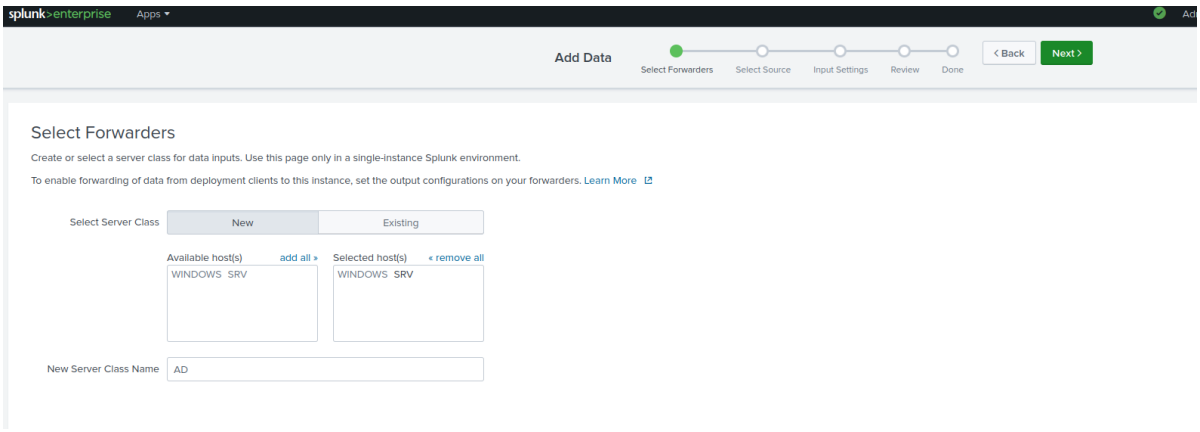
1. **Setting** -> **Add Data**



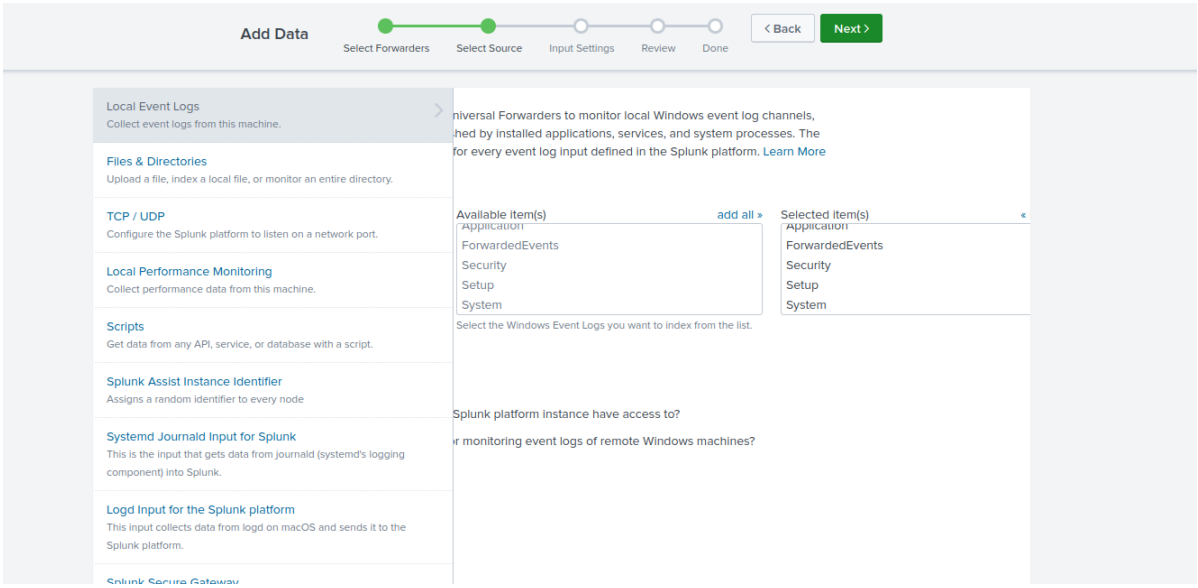
2. Choose **Forward**



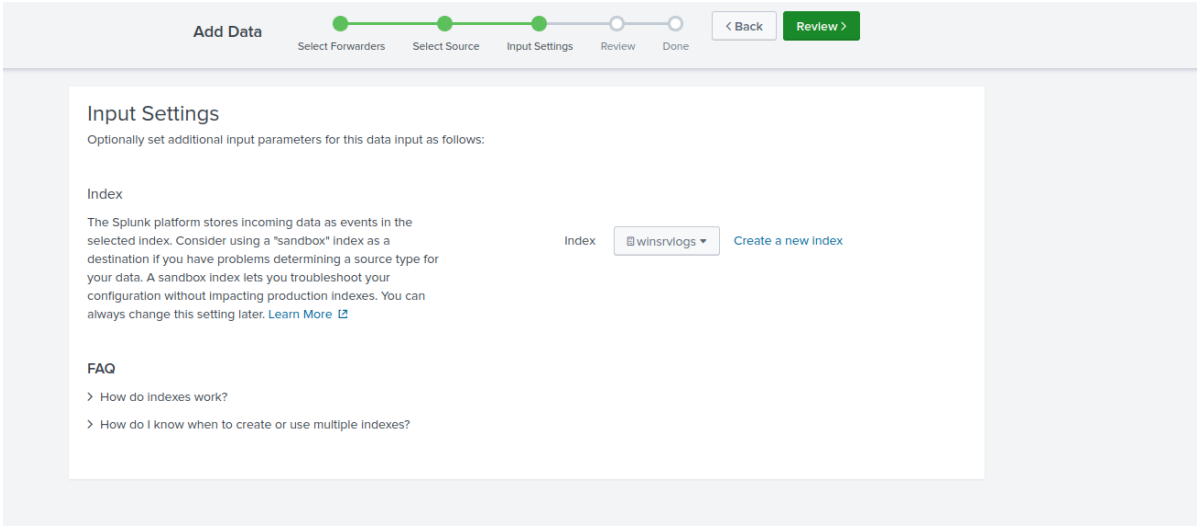
3. Select host **Windows SRV**, input **New Server Class Name** and Next

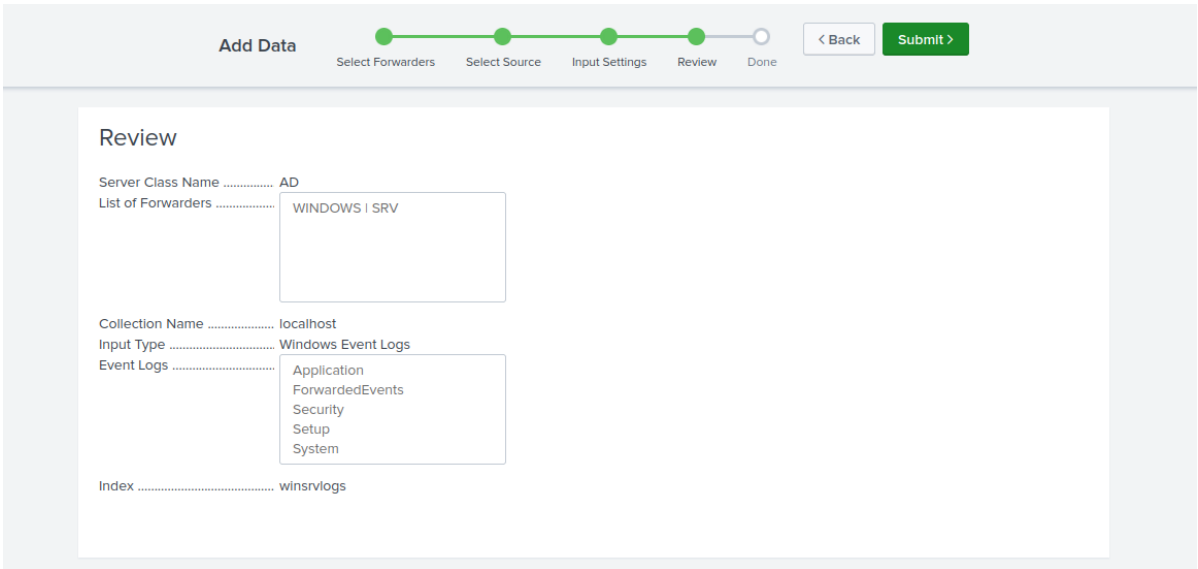


4. **Local Event Logs** -> **add all**

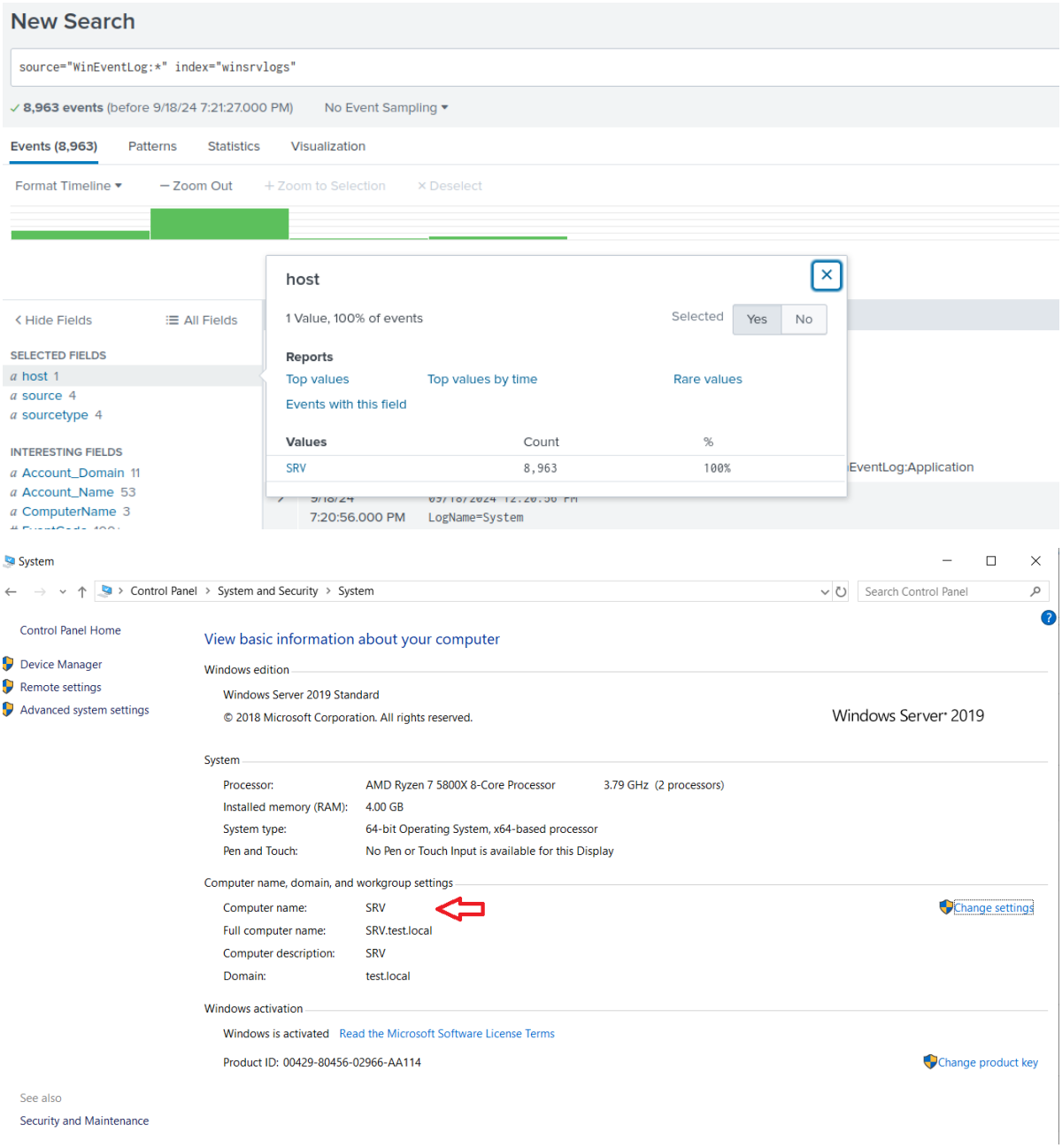


5. **index** -> **winsrvlogs**

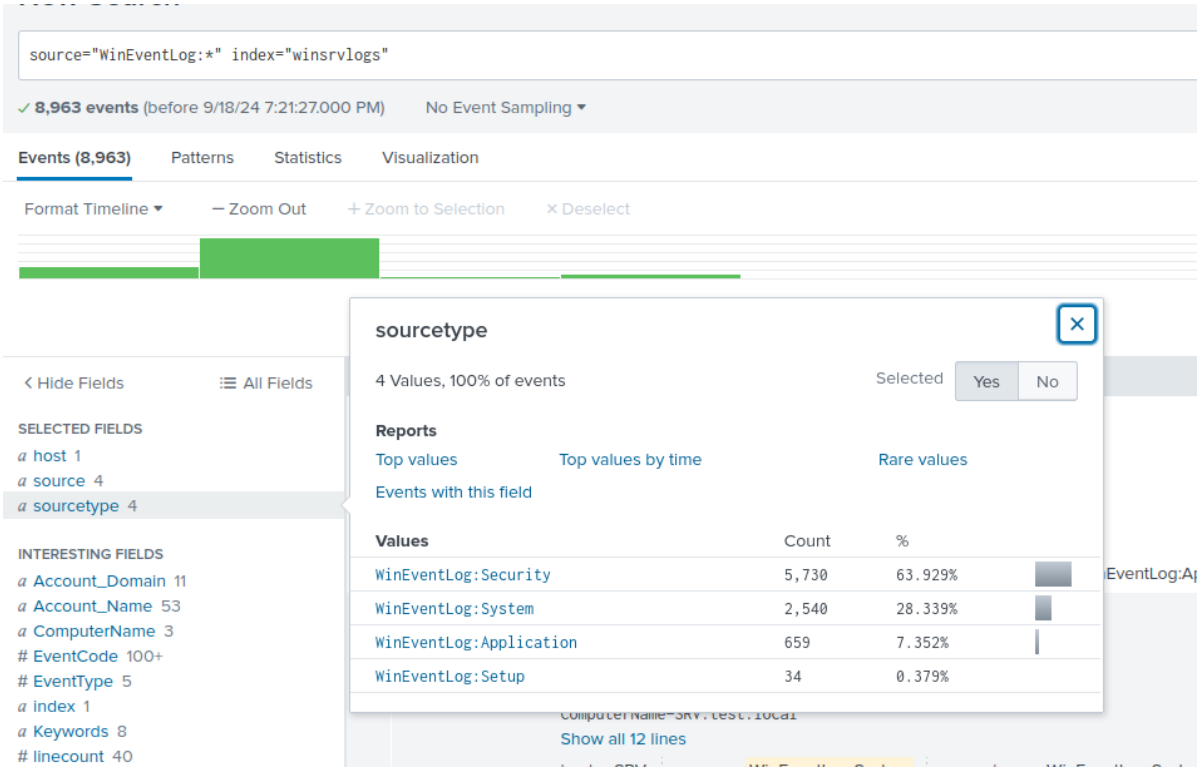


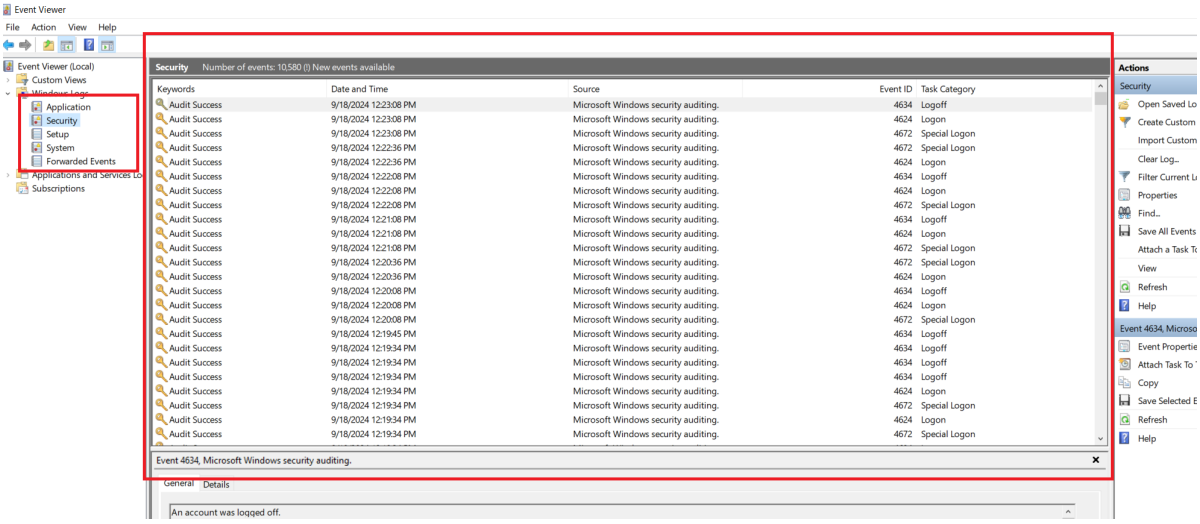


6. Now Windows Server host has shown up in Splunk



Also, Windows Server Local Event Logs has been forwarded to Splunk


source="WinEventLog:*" index="winsrvlogs"
8,963 events (before 9/18/24 7:21:27.000 PM)
No Event Sampling
Events (8,963)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 4
a sourcetype 4
INTERESTING FIELDS
a Account_Domain 11
a Account_Name 53
a ComputerName 3
EventCode 100+
EventType 5
a index 1
a Keywords 8
linecount 40
sourcetype
4 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
WinEventLog:Security
5,730
63.929%
WinEventLog:System
2,540
28.339%
WinEventLog:Application
659
7.352%
WinEventLog:Setup
34
0.379%
Show all 12 lines


Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Subscriptions
Security
Number of events: 10,580 (!) New events available
Keywords
Date and Time
Source
Event ID
Task Category
Audit Success
9/18/2024 12:23:08 PM
Microsoft Windows security auditing.
4634
Logoff
4624
Logon
4672
Special Logon
Event 4634, Microsoft Windows security auditing.
General
Details
An account was logged off.
Actions
Security
Open Saved Lo
Create Custom
Import Custom
Clear Log...
Filter Current L
Properties
Find...
Save All Events
Attach a Task To
View
Refresh
Help
Event 4634, Microso
Event Properties
Attach Task To
Copy
Save Selected E
Refresh
Help