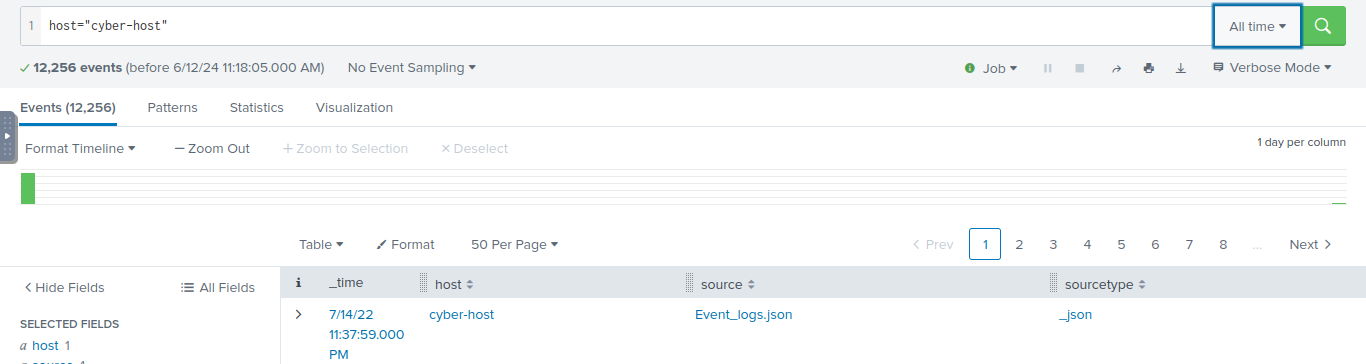
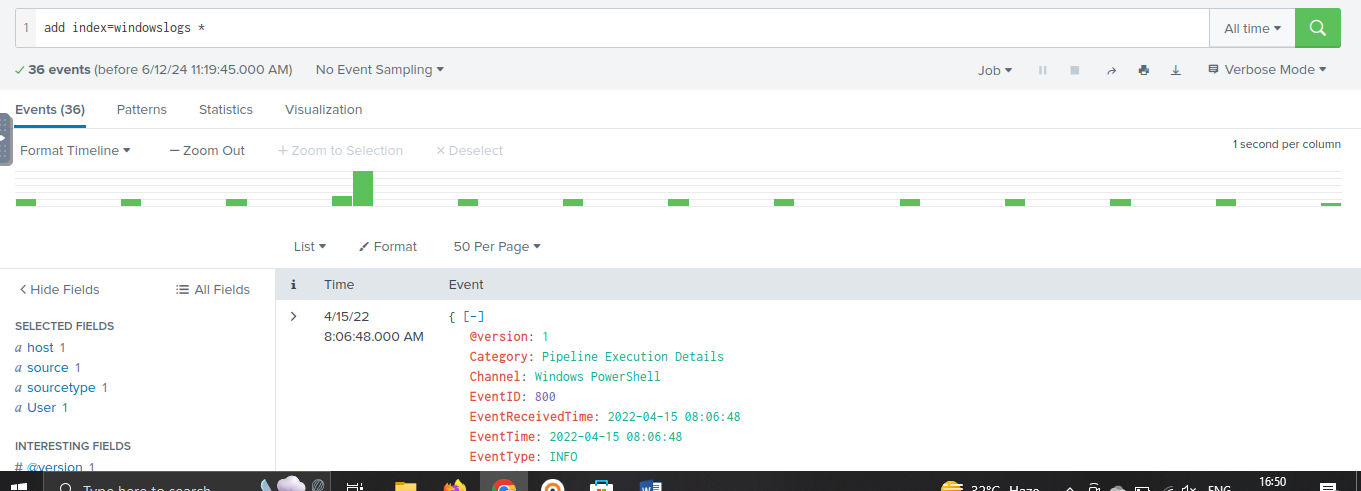
Exploring Splunk

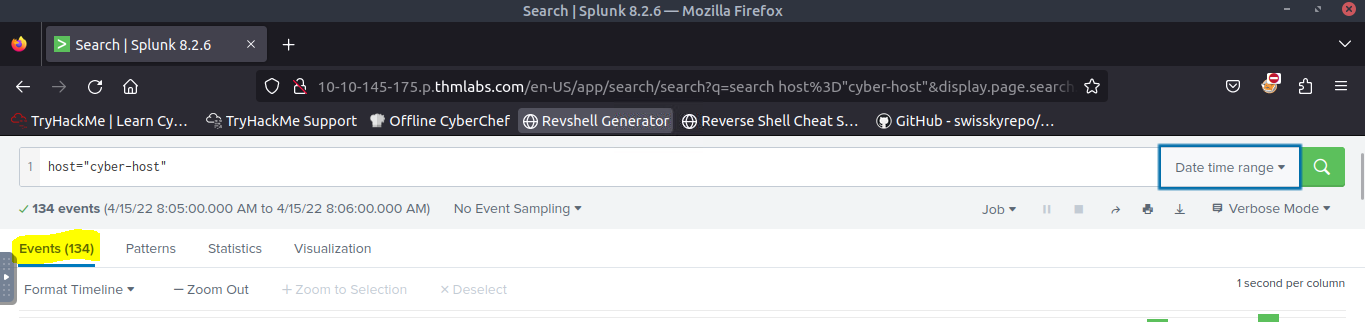
Total events for the host for all time is:



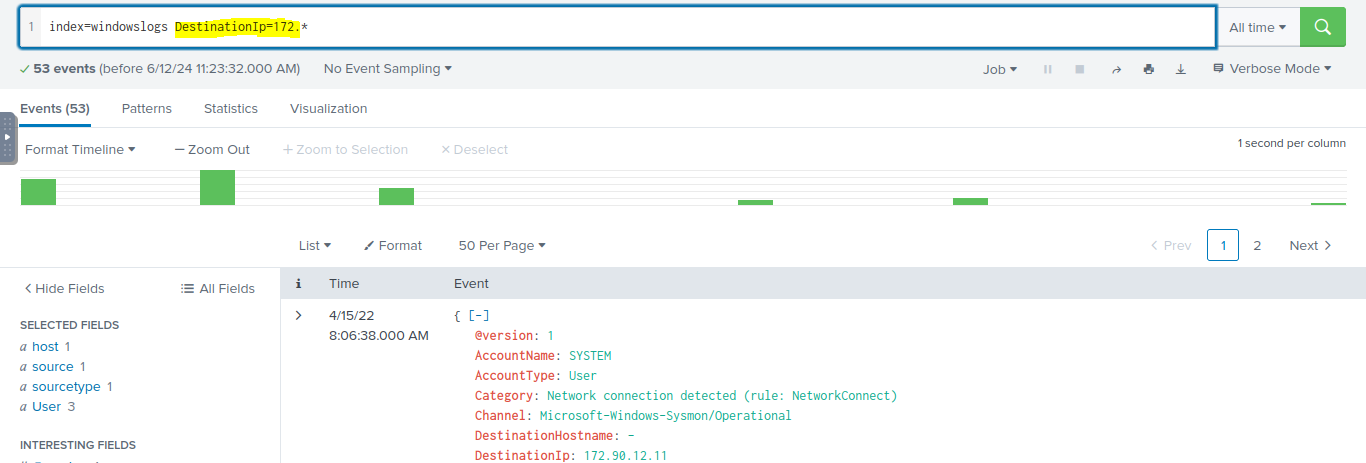
Working specifically on index = windows logs



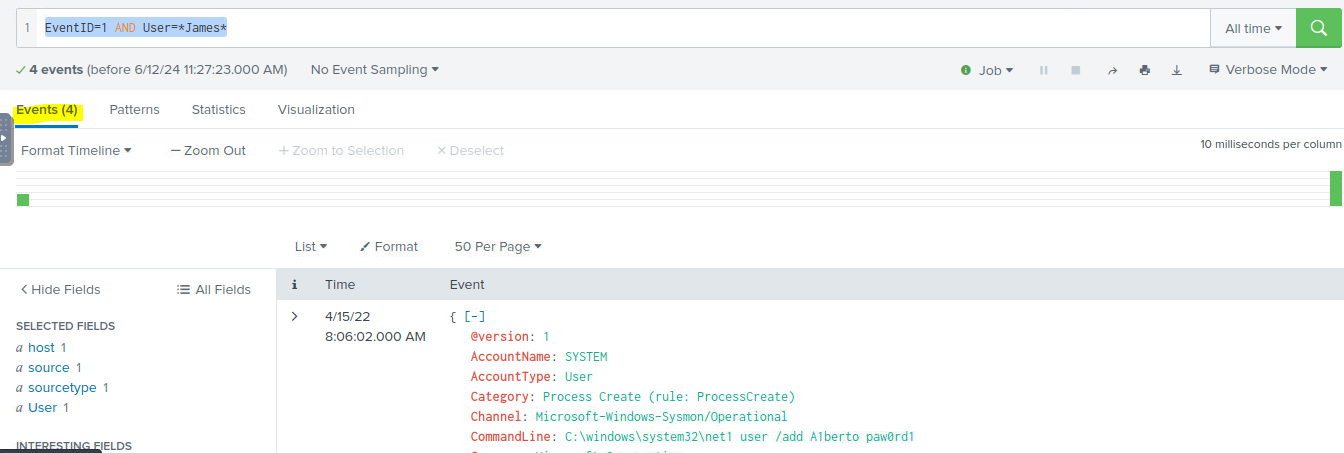
Searching for number of events during a time period between 8:05 am to 8:06 am on 4/15/2022.



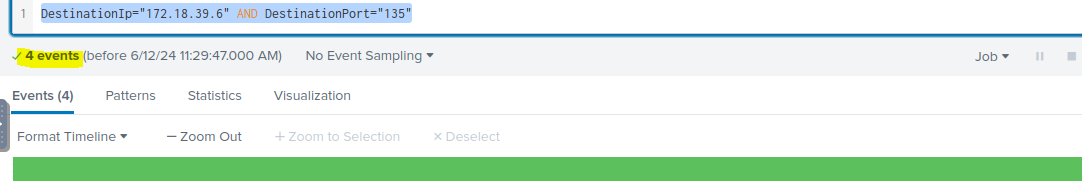
Using wildcard to search ips starting with 172



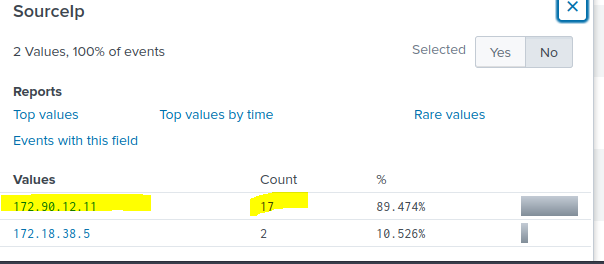
searching for Event ID 1 **AND** User as \*James\*



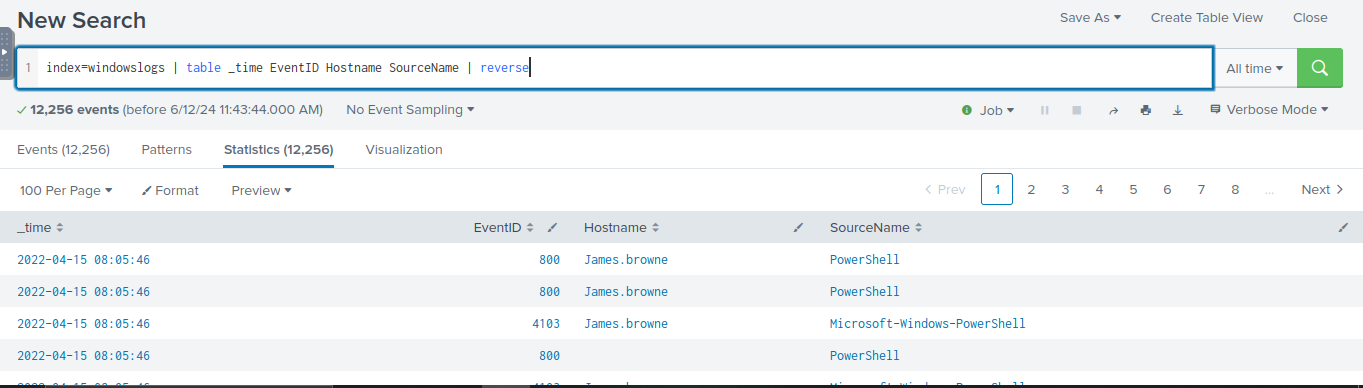
vents are observed with Destination IP 172.18.39.6 AND destination Port 135



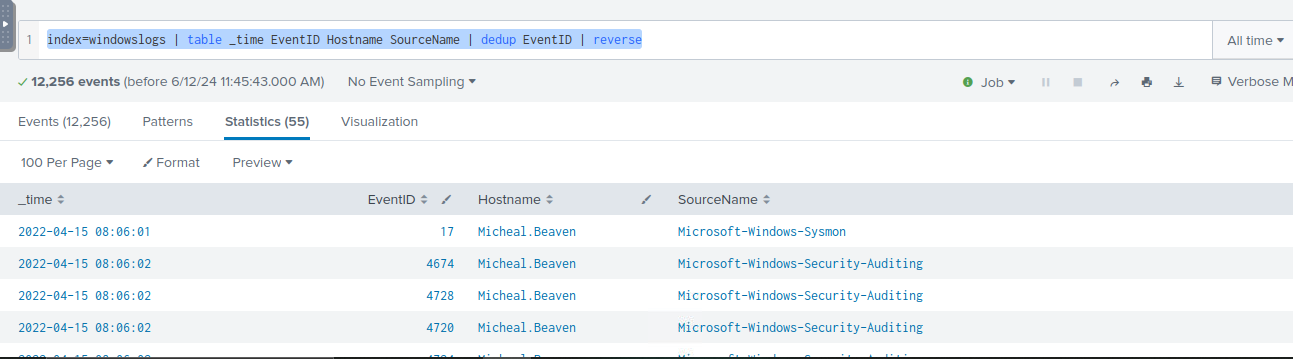
 index=windowslogs  Hostname="Salena.Adam" DestinationIp="172.18.38.5" . Which ip initiates more to the destination in this instance?



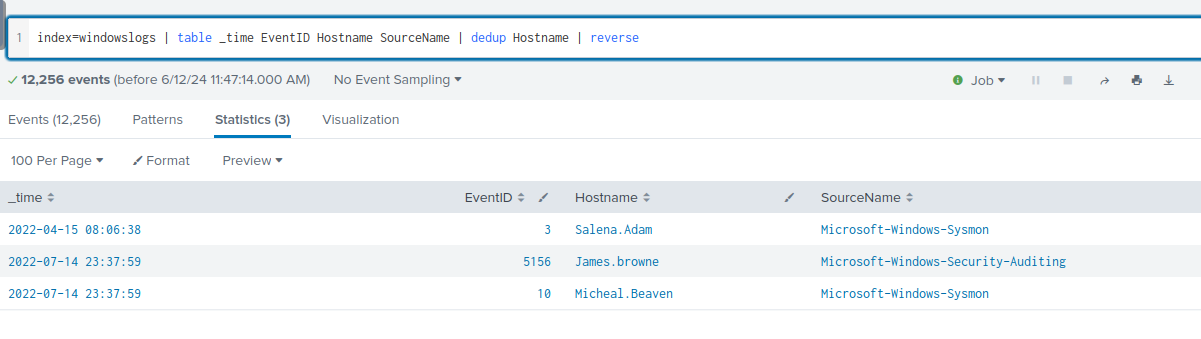
index=windowslogs | table \_time EventID Hostname SourceName | reverse



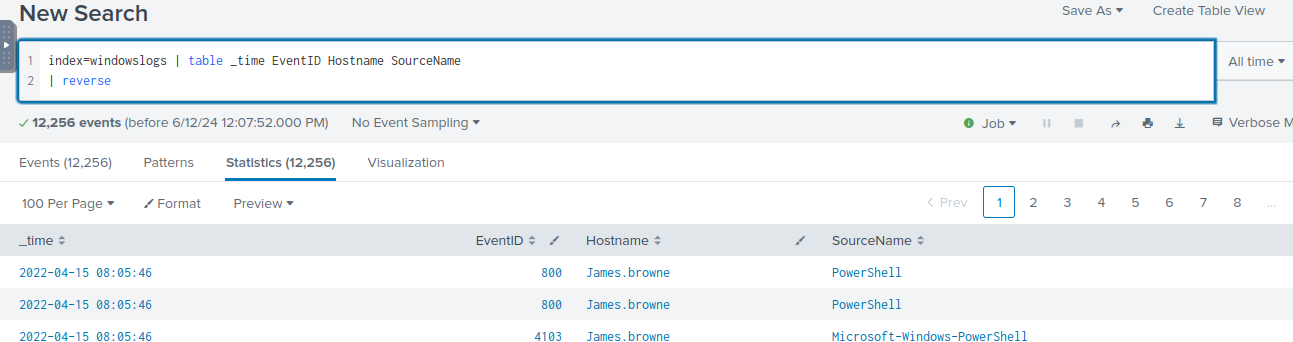
index=windowslogs | table \_time EventID Hostname SourceName | dedup EventID | reverse



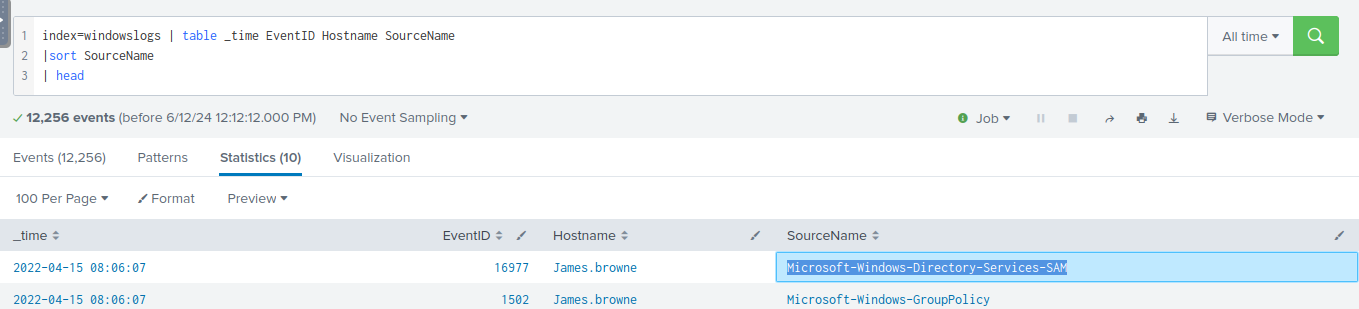
index=windowslogs | table \_time EventID Hostname SourceName | dedup Hostname | reverse



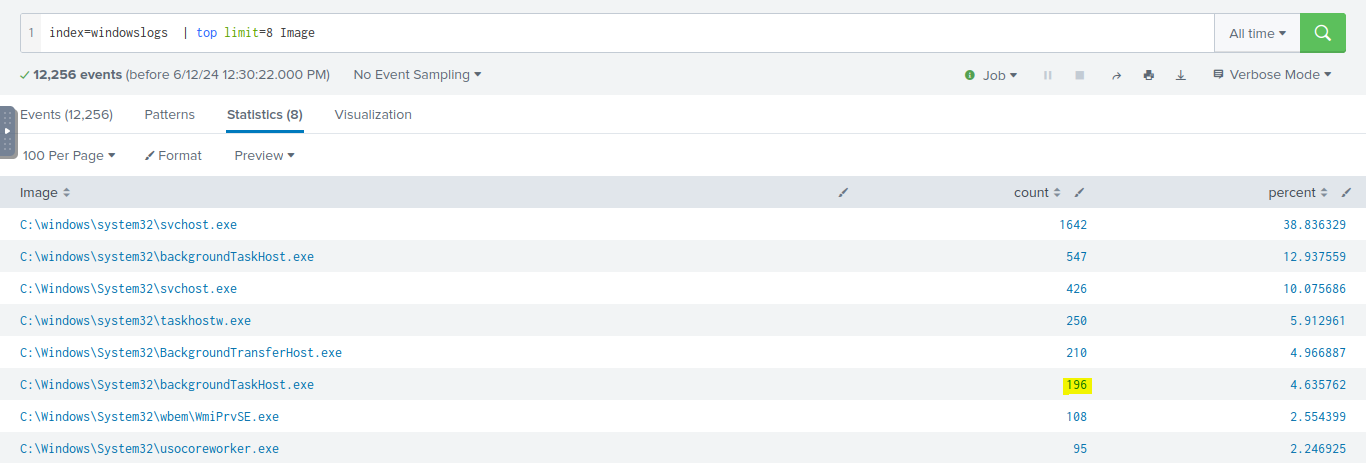
Reverse of the list and its host name



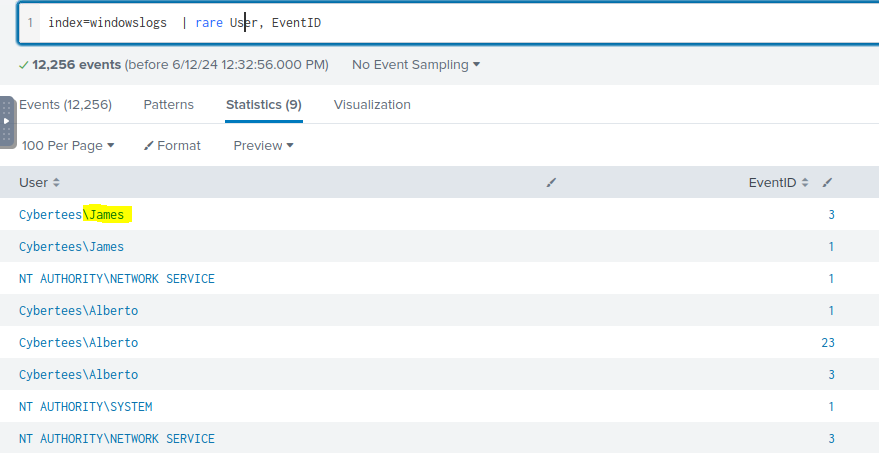
The top of the list when sorted.



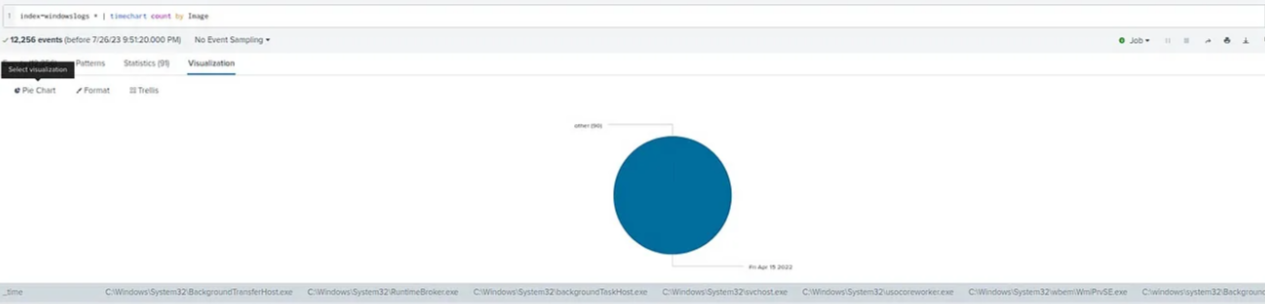
Total count of 6th image in the top 8 limit of the images



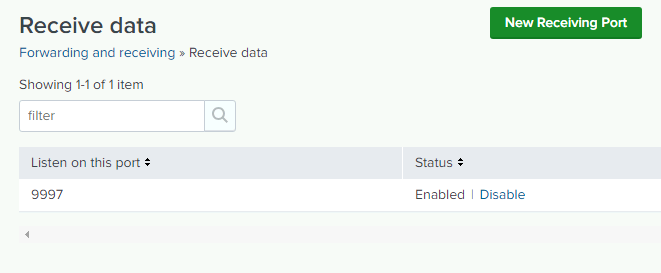
The user with the least number of activities



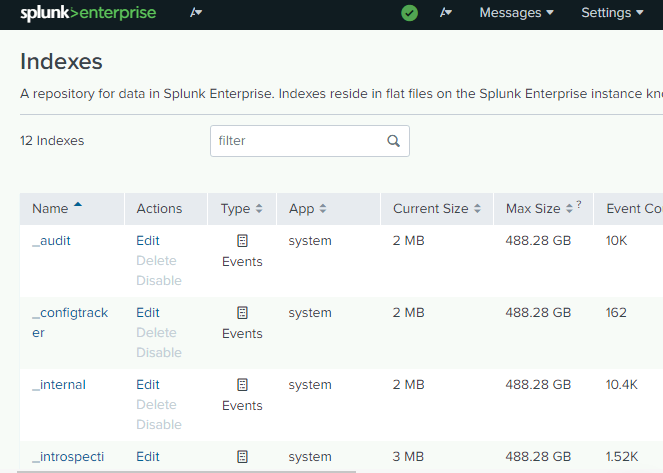
Piechart visualization



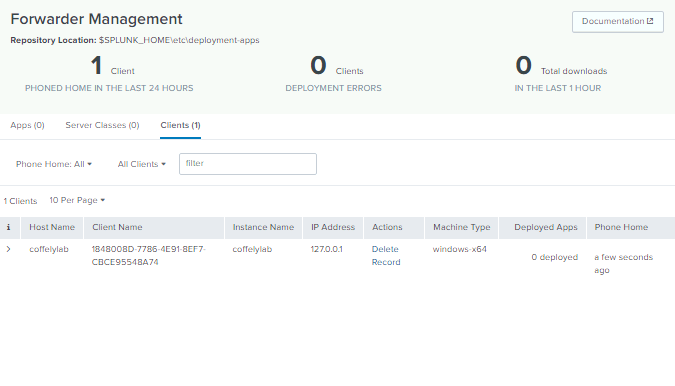
Rceiving data. Listening on port 9997



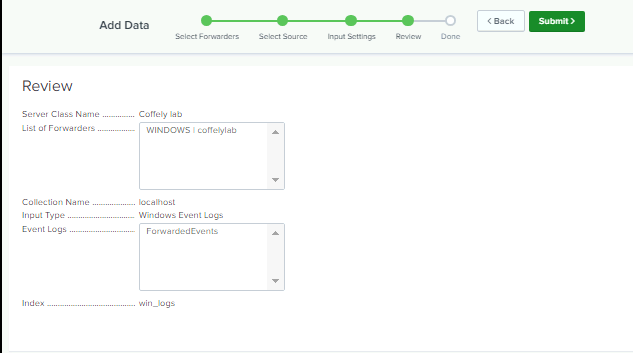
Indexes



Forwarder management



Configure forwarder



Weblog data

