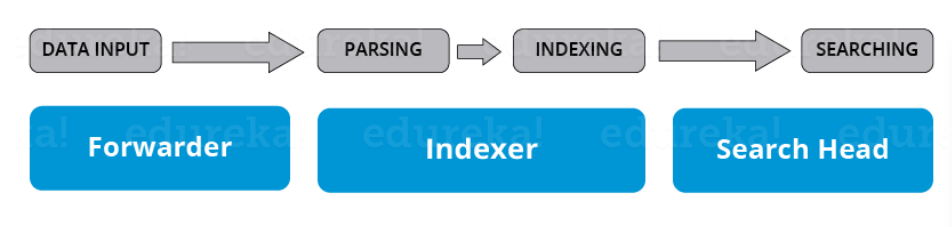
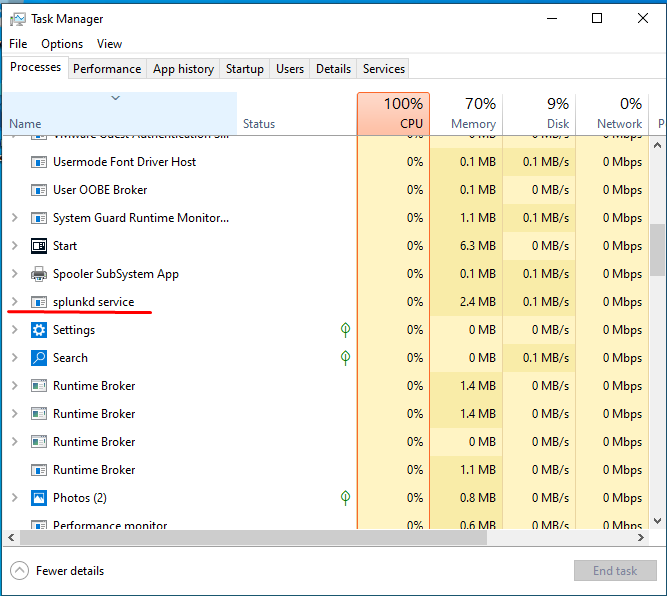
Mô hình triển khai splunk



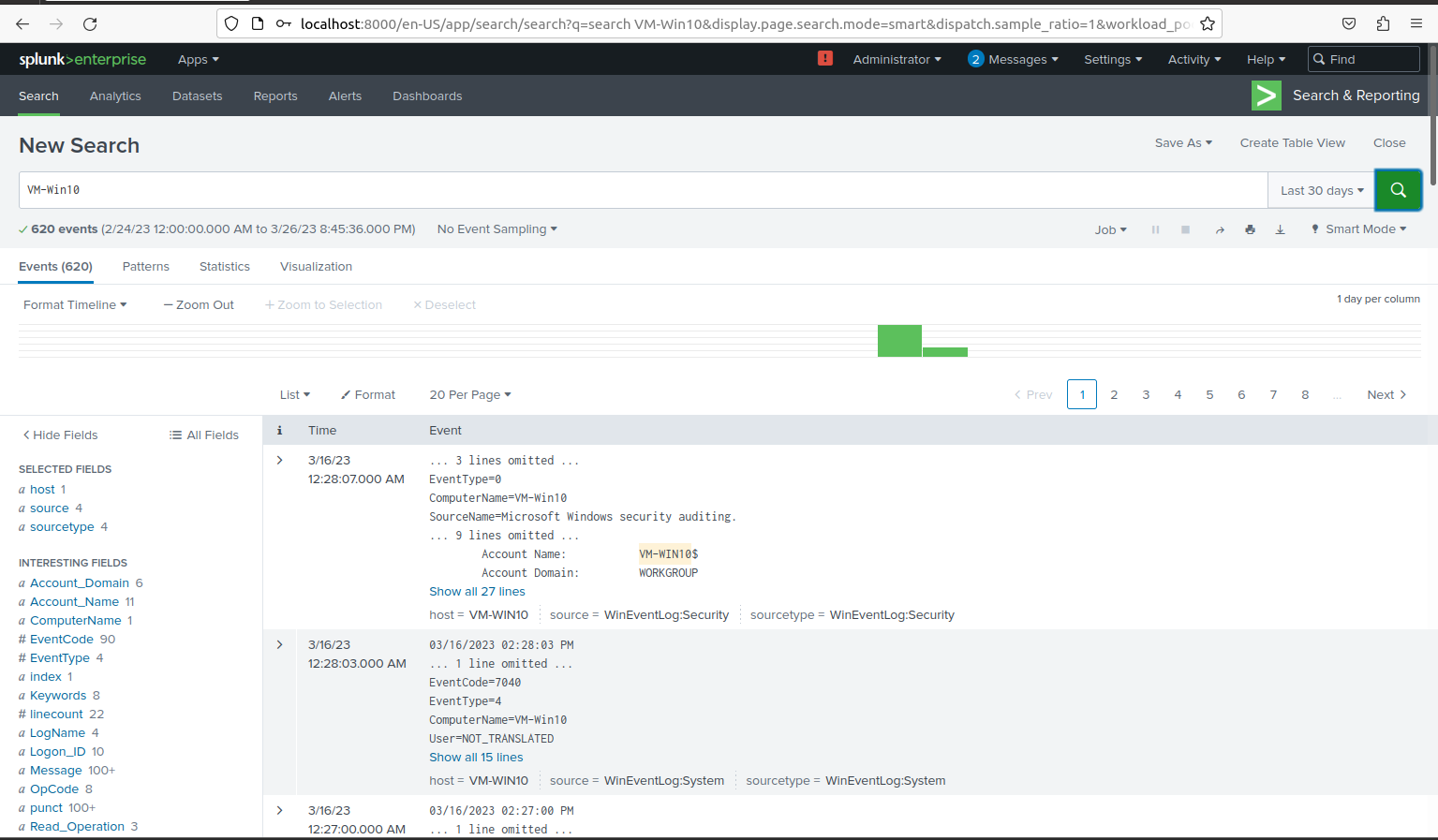
**Search Head**: Splunk cài đặt trên Ubuntu 20.04

**Forwarder**: Windows 10 Cài đặt UniversalForwarder và đổi tên là VM-Win10

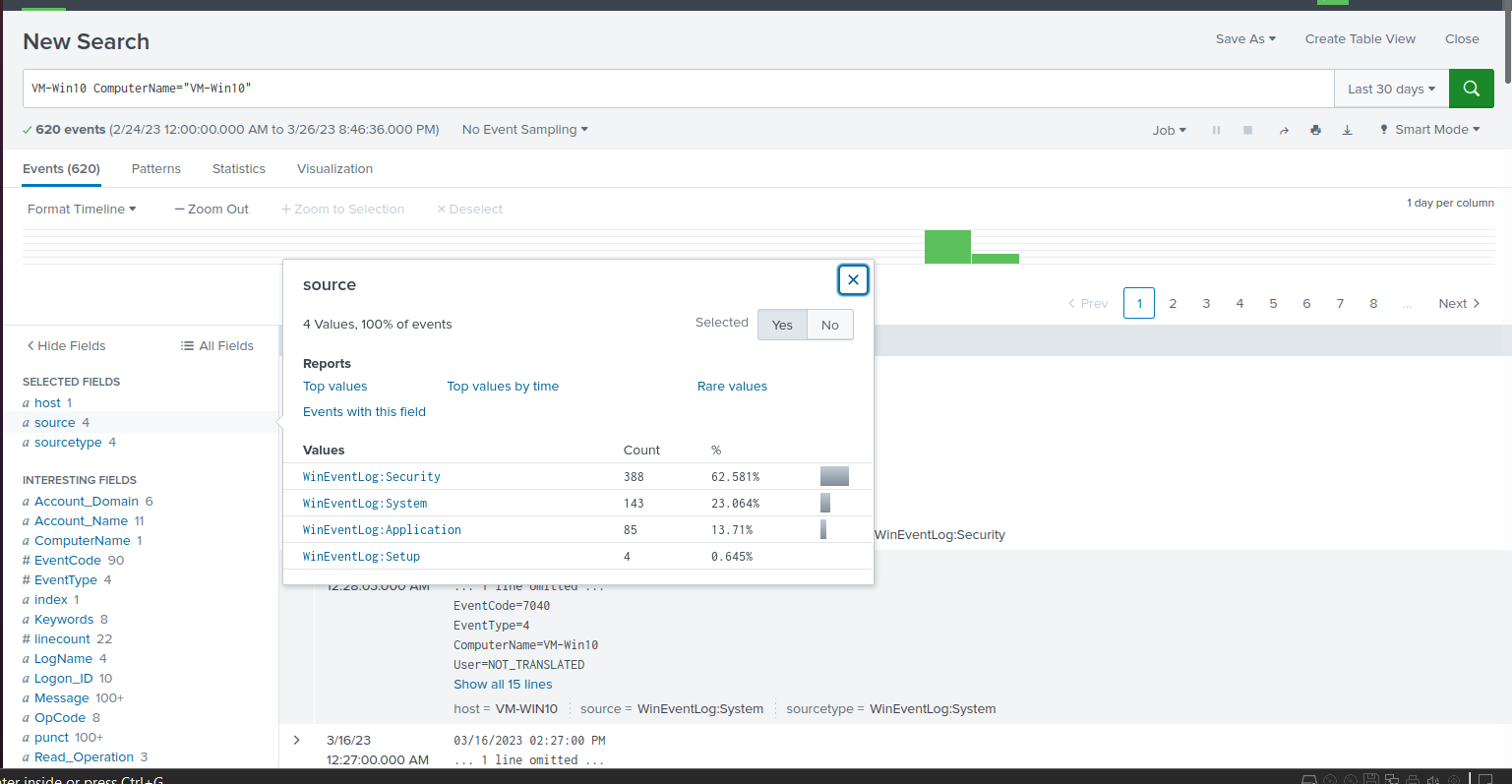
Sau khi cài đặt xong universalForwarder thì mỗi khi khởi động windows, splunk cũng sẽ khởi động theo.



Giao diện ô search log trên splunk



Search theo source log:



Search theo Account\_Name

