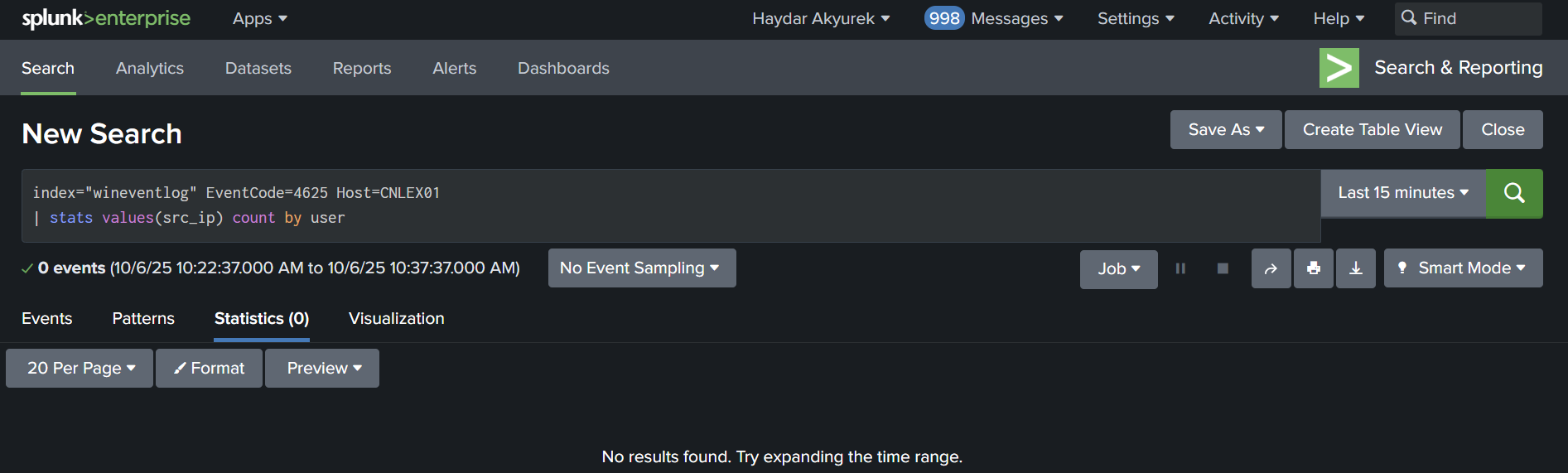
**Windows LOGS**

1. List the users and external IP addresses that have failed to log in to the Exchange machine security logs in the last 15 minutes.

**index="wineventlog" EventCode=4625 Host=CNLEX01**

**| stats values(src\_ip) count by user**

****

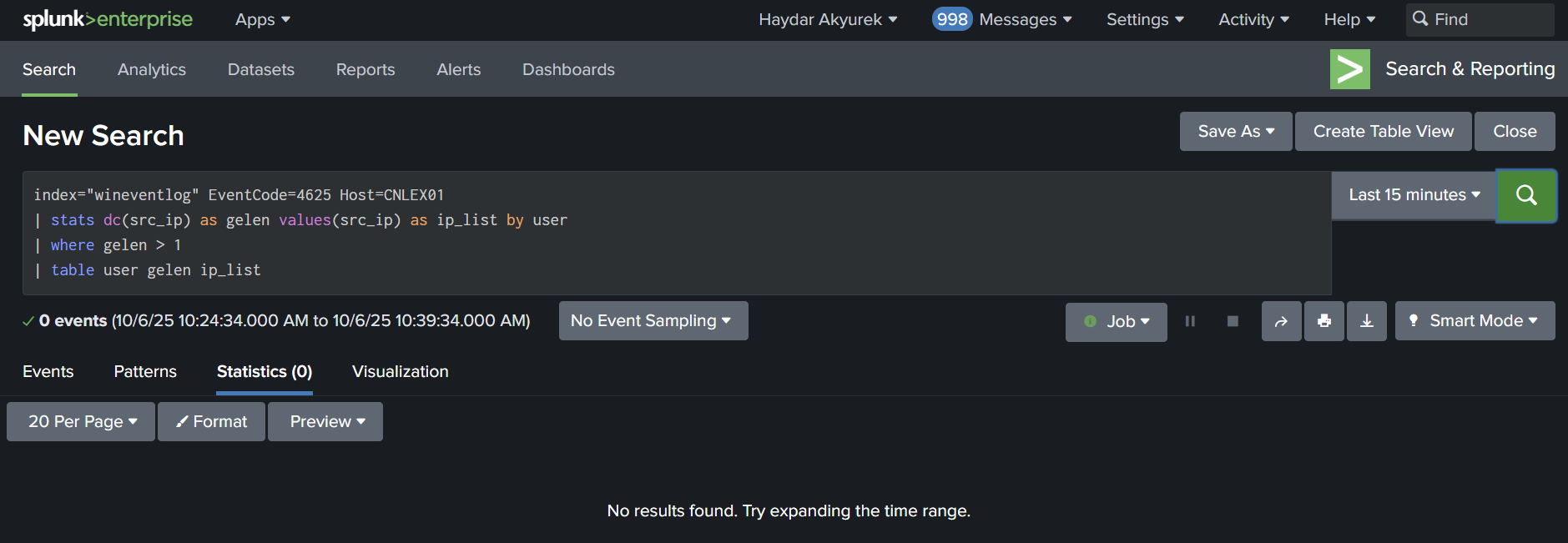
**2.** List users who have unsuccessfully logged in with more than one external IP address in the Exchange machine security logs in the last 15 minutes.

**index="wineventlog" EventCode=4625 Host=CNLEX01**

**| stats dc(src\_ip) as gelen values(src\_ip) as ip\_list by user**

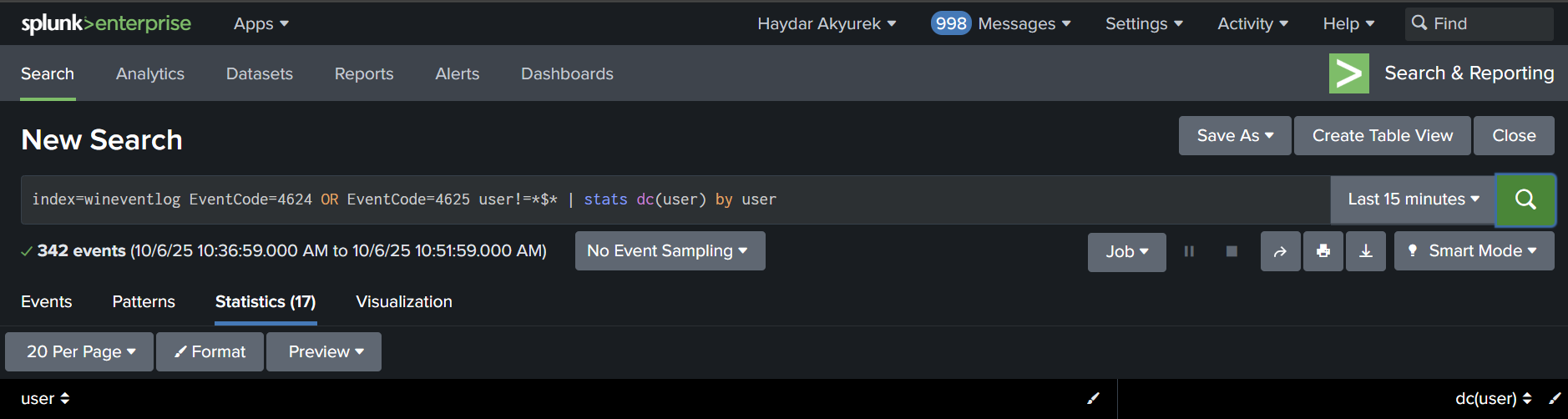
**| where gelen > 1**

**| table user gelen ip\_list**



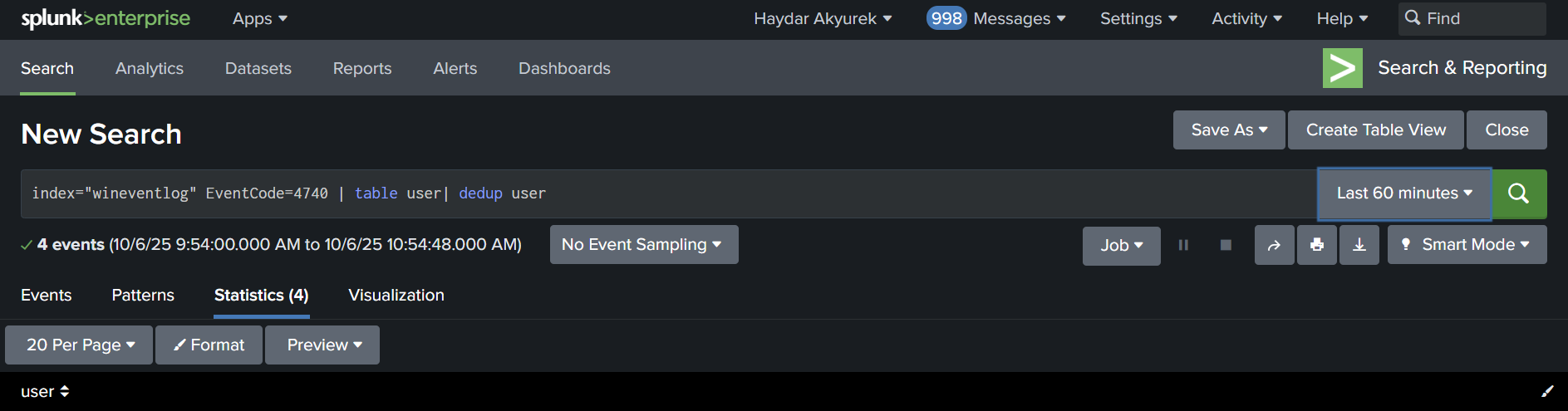
**3.** List successful and unsuccessful logins from the same user in the Windows security logs in the last 15 minutes.

**index=wineventlog EventCode=4624 OR EventCode=4625 user!=\*$\* | stats dc(user) by user**

****

**4.** List users whose accounts have been locked in the Windows security logs in the last 24 hours.

**index="wineventlog" EventCode=4740 | table user| dedup user**

****