Splunk Drill Down Events

```
earliest=$initial_time$ latest=$end_time$ index=$index$ EventCode=4624 NOT Logon_Type IN ("5")
host=$orig_host$
```

> orig_action_name
> orig_host
> orig_rid
> orig_sid

Revision #1
Created 2022-03-23 17:01:58 UTC by Clinton
Updated 2022-03-23 17:03:40 UTC by Clinton