

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 23 March 2022 17:01:58 by Clinton

Updated 23 March 2022 17:03:40 by Clinton