

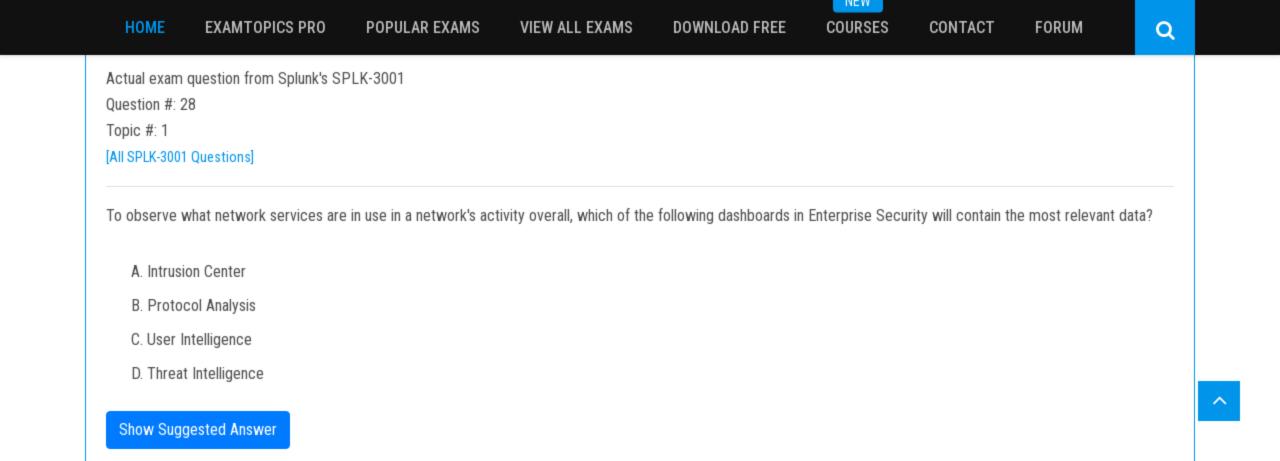
[All SPLK-3001 Questions]

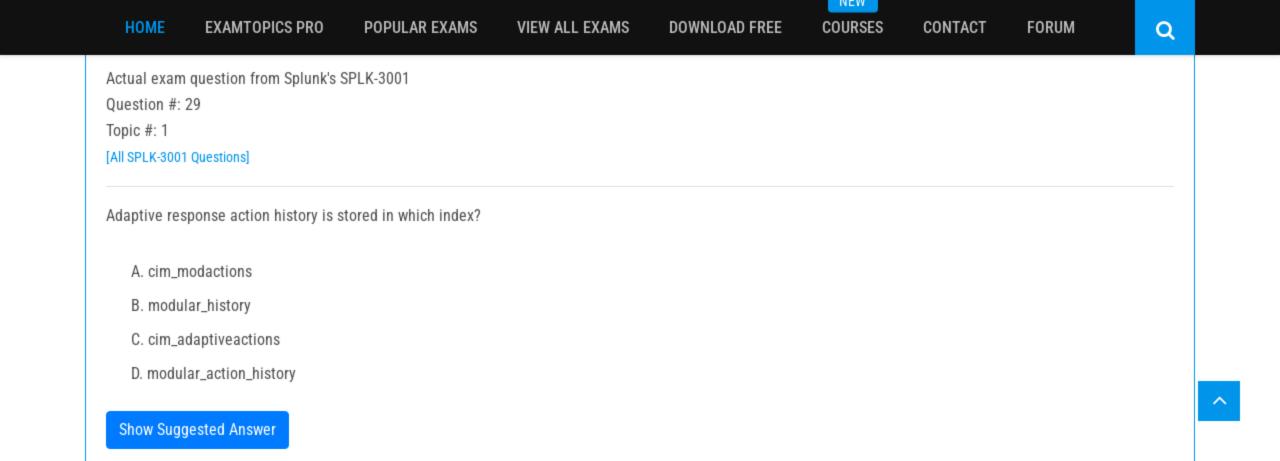
An administrator is asked to configure an 'Nslookup' adaptive response action, so that it appears as a selectable option in the notable event's action menu when an analyst is working in the Incident Review dashboard.

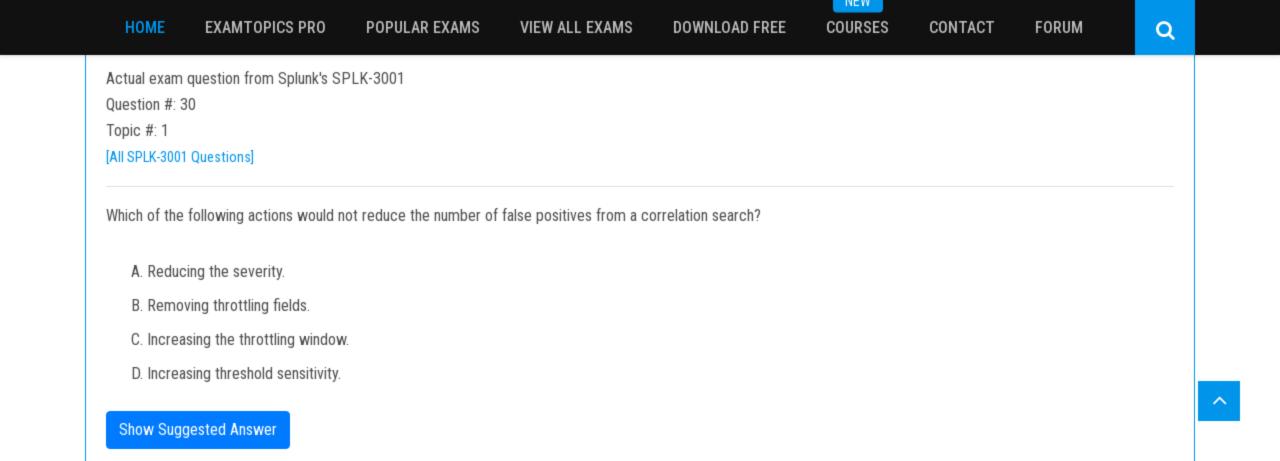
What steps would the administrator take to configure this option?

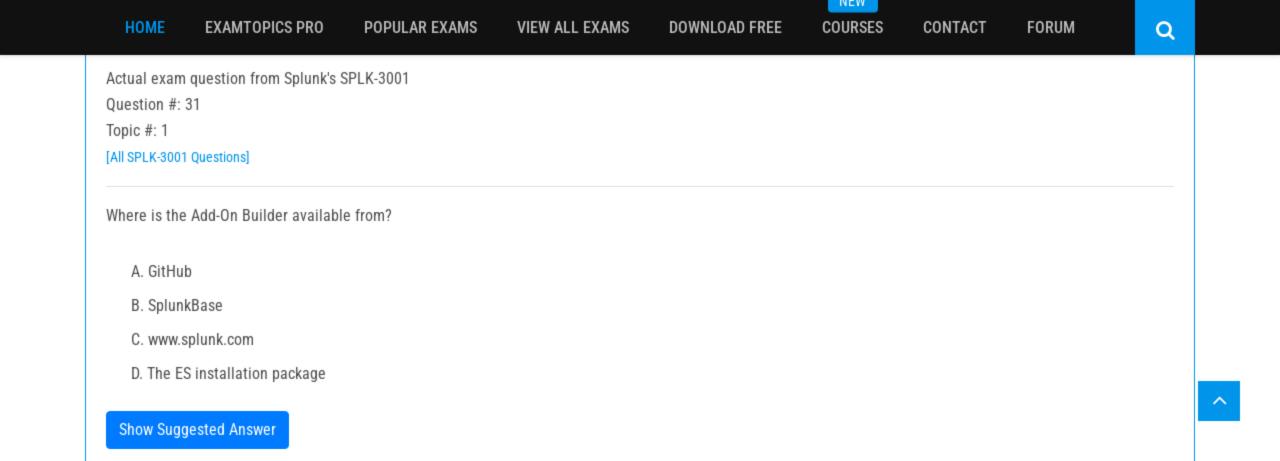
- A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup
- B. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
- C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
- D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

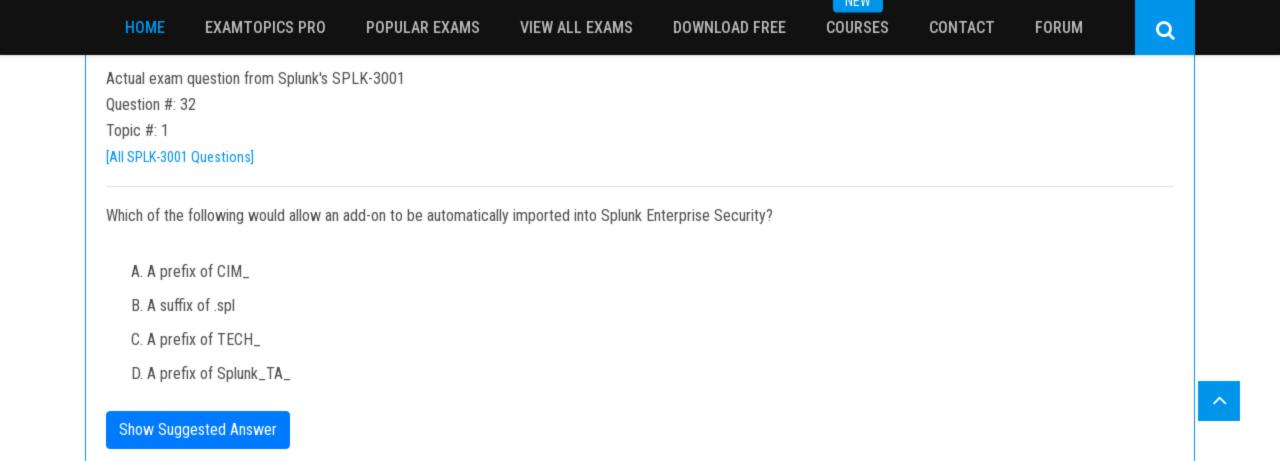
**Show Suggested Answer** 

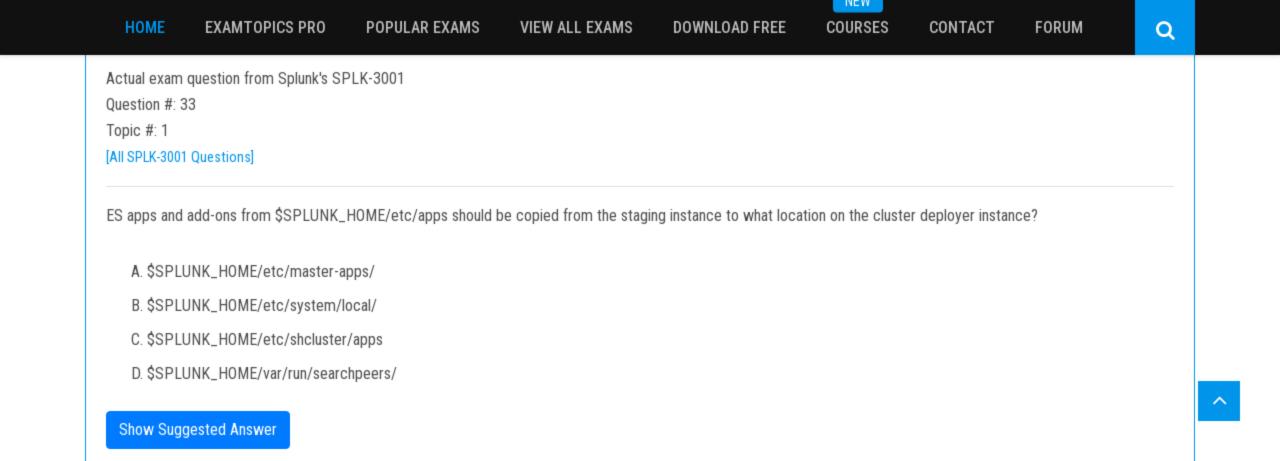












HOME EXAMTOPICS PRO POPULAR EXAMS VIEW ALL EXAMS DOWNLOAD FREE COURSES CONTACT FORUM Q

IAC AA

Actual exam question from Splunk's SPLK-3001

Question #: 35

Topic #: 1

[All SPLK-3001 Questions]

What kind of value is in the red box in this picture?

## Additional Fields Value

HTTP Method

GET

Source

10.98.27.195 500

Source Expected false
Source PCI Domain untrust
Source Requires Antivirus false
Source Should Time Synchronize false
Source Should Update false

Tag modaction\_result

- A. A risk score.
- B. A source ranking.
- C. An event priority.
- D. An IP address rating.

**Show Suggested Answer** 

