# SPLK-1003 Q&As

Splunk Enterprise Certified Admin

## Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.passapply.com/splk-1003.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

Which of the following must be done to define user permissions when integrating Splunk with LDAP?

A. Map Users

B. Map Groups

C. Map LDAP Inheritance

D. Map LDAP to Active Directory

Correct Answer: B

"You can map either users or groups, but not both. If you are using groups, all users must be members of an appropriate group. Groups inherit capabilities form the highest level role they\\'re a member of." "If your LDAP environment does not have group entries, you can treat each user as its own group."

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/ConfigureLDAPwithSplunkWeb

**QUESTION 2**

Which Splunk forwarder type allows parsing of data before forwarding to an indexer?

A. Universal forwarder

B. Parsing forwarder

C. Heavy forwarder

D. Advanced forwarder

Correct Answer: C

**QUESTION 3**

An organization wants to collect Windows performance data from a set of clients, however, installing Splunk software on these clients is not allowed. What option is available to collect this data in Splunk Enterprise?

A. Use Local Windows host monitoring.

B. Use Windows Remote Inputs with WMI.

C. Use Local Windows network monitoring.

D. Use an index with an Index Data Type of Metrics.

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/ConsiderationsfordecidinghowtomonitorWindowsdata

"The Splunk platform collects remote Windows data for indexing in one of two ways: From Splunk forwarders, Using Windows Management Instrumentation (WMI). For Splunk Cloud deployments, you must use the Splunk Universal Forwarder on a Windows machines to montior remote Windows data."

**QUESTION 4**

Which option on the Add Data menu is most useful for testing data ingestion without creating inputs.conf?

A. Upload option

B. Forward option

C. Monitor option

D. Download option

Correct Answer: A

**QUESTION 5**

Which Splunk component does a search head primarily communicate with?

A. Indexer

B. Forwarder

C. Cluster master

D. Deployment server

Correct Answer: A