Bộ câu hỏi luyện thi Splunk Power User và Splunk Admin (Câu 1-150)

Câu 1: Trong Splunk, để theo dõi hiệu suất của các tìm kiếm, bạn xem log nào?

* A. scheduler.log
* B. splunkd.log
* C. metrics.log
* D. audit.log

Đáp án: A

Câu 2: Lệnh nào dùng để tìm kiếm sự kiện có chứa từ khóa "error"?

* A. search error
* B. find error
* C. locate error
* D. get error

Đáp án: A

Câu 4: Lệnh Splunk nào để đếm số lượng sự kiện?

* A. stats count
* B. count events
* C. sum events
* D. total events

Đáp án: A

Câu 7: Lệnh Splunk nào dùng để nhóm dữ liệu theo trường cụ thể?

* A. stats count by field
* B. group by field
* C. cluster field
* D. sort by field

Đáp án: A

Câu 8: Bạn muốn loại bỏ các sự kiện trùng lặp trong kết quả tìm kiếm, dùng lệnh nào?

* A. dedup
* B. unique
* C. distinct
* D. remove duplicates

Đáp án: A

Câu 9: Trong Splunk, để chuyển đổi dữ liệu thô thành các trường có thể tìm kiếm, bạn dùng gì?

* A. Field Extraction
* B. Data Model
* C. Search Command
* D. Dashboard

Đáp án: A

Câu 10: Bạn muốn gửi cảnh báo qua email, phải cấu hình gì?

* A. Alert Action
* B. Alert Trigger
* C. Alert Condition
* D. Alert Schedule

Đáp án: A

Câu 155: Bạn muốn tạo một cảnh báo để tự động chạy một script khi có sự kiện nhất định, bạn chọn Alert action nào?

* A. Run a script
* B. Send email
* C. Webhook
* D. Log event

Đáp án: A

Câu 156: Lệnh Splunk nào được sử dụng để lọc sự kiện chỉ chứa lỗi (error) và cảnh báo (warn)?

* A. search error OR warn
* B. search error AND warn
* C. where status="error" OR status="warn"
* D. stats error OR warn

Đáp án: A

Câu 157: Bạn muốn kết hợp hai bảng dữ liệu bằng cách thêm các sự kiện của bảng thứ hai vào bảng đầu, dùng lệnh?

* A. append
* B. join
* C. union
* D. lookup

Đáp án: A

Câu 158: Khi triển khai Splunk Search Head Cluster, thành phần nào đảm nhiệm cân bằng tải tìm kiếm?

* A. Load Balancer
* B. Deployment Server
* C. Indexer
* D. Search Head Captain

Đáp án: A

Câu 160: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 170: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 180: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 190: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 200: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Câu 210: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 220: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 230: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 240: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A  
  
  
Câu 250: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 260: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 270: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 280: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 289: Bạn muốn tạo trường mới `duration\_minutes` tính từ trường `duration\_seconds` (tính theo giây), lệnh Splunk nào đúng?

* A. eval duration\_minutes = duration\_seconds / 60
* B. eval duration\_minutes = duration\_seconds \* 60
* C. eval duration\_minutes = duration\_seconds % 60
* D. eval duration\_minutes = duration\_seconds + 60

Đáp án: A

Câu 290: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A

Câu 300: Bạn muốn ghi lại mọi thao tác người dùng trong Splunk để phục vụ kiểm tra bảo mật, log nào là phù hợp nhất?

* A. audit.log
* B. splunkd.log
* C. metrics.log
* D. scheduler.log

Đáp án: A