642-544

(Implementing Cisco Security Monitoring, Analysis and Response)

Document version:1 04 11

Important Note About 642-544 PDF

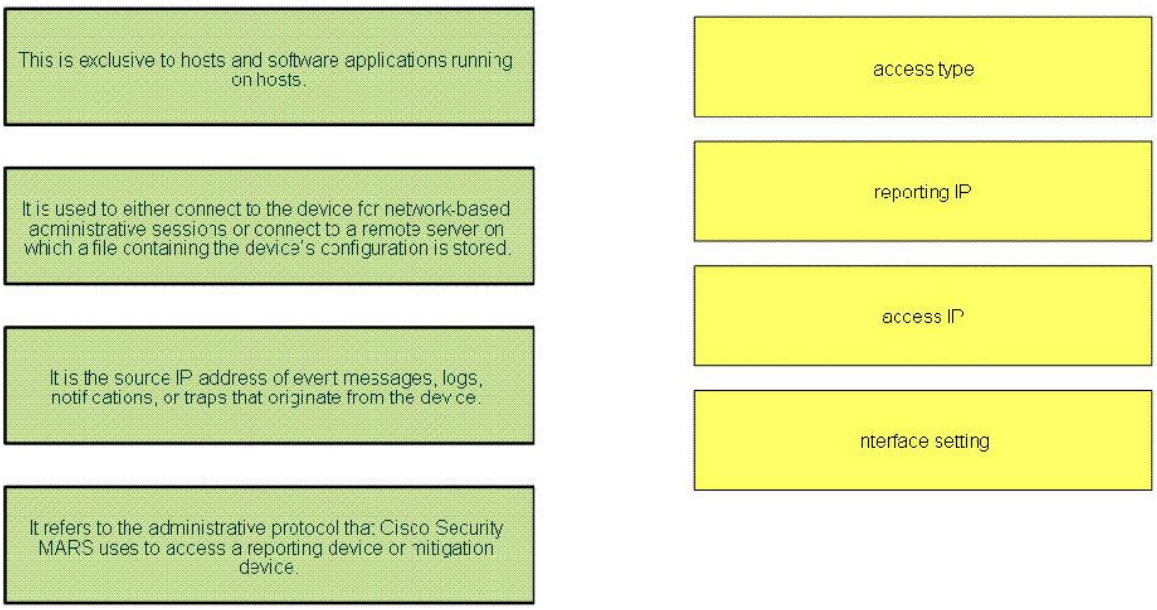
techeXams' 642-544 **PDF** is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this exam questions. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. It's our guarantee.

Copyright

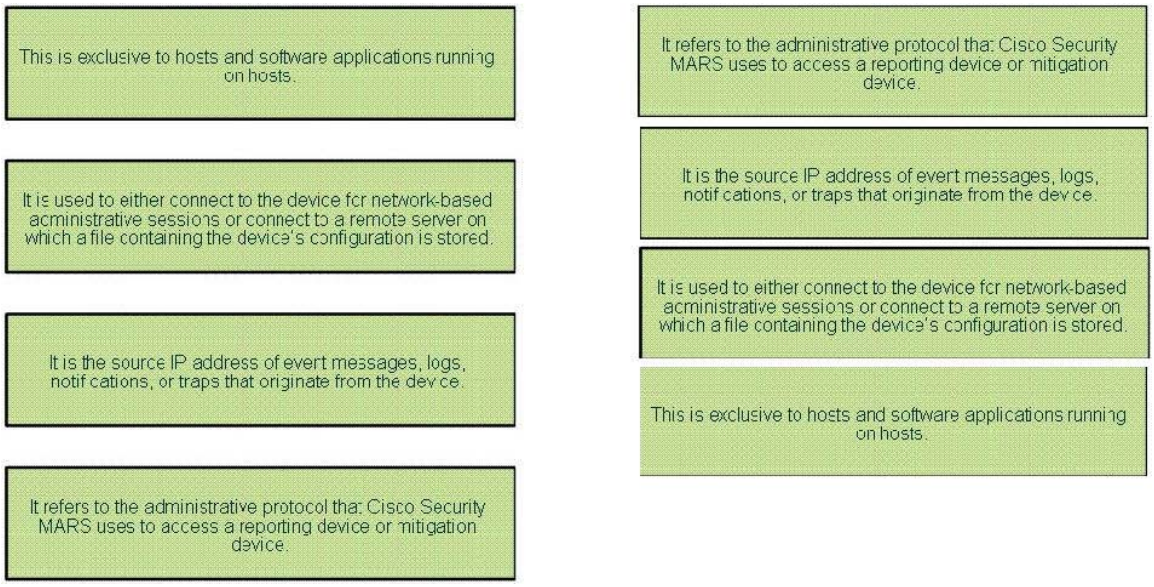
Disclaimer

Question: 1

The definitions on the left to the appropriate terms on the right



Answer:



Question: 2

What will happen if you try to run a Cisco Security MARS query that will take a long time to complete?

A. After submitting the query, the Cisco Security MARS GUI screen will be locked up until the query is completed.
B. The query will be automatically saved as a rule.
C. The query will be automatically saved as a report.
D. You will be prompted to "Submit Batch" to run the query in batch mode.

Answer: D

Question: 3

The Cisco Security MARS appliance supports which protocol for data archiving and restoring?

A. NFS
B. TFTP
C. FTP
D. Secure FTP
E. SSH

Answer: A

Question: 4

What is a benefit of using the dollar variable (as in $TARGET01) when creating queries in Cisco Security MARS?

A. The dollar variable enables multiple queries to reference the same common 5-tuple information using a variable.
B. The dollar variable ensures that the probes and attacks that are reported are happening to the same host.
C. The dollar variable allows matching of any unknown reporting device.
D. The dollar variable allows matching of any event type groups.
E. The dollar variable enables the same query to be applied to different reports.
F. The dollar variable enables the same query to be applied to different cases.

Answer: B

Question: 5

A Cisco Security MARS appliance cannot access certain devices through the default gateway. Troubleshooting has determined that this is a Cisco Security MARS configuration issue. Which additional Cisco Security MARS configuration will be required to correct this issue?

A. Use the Cisco Security MARS GUI or CLI to enable a dynamic routing protocol
B. Use the Cisco Security MARS CLI to add a static route
C. Use the Cisco Security MARS GUI to configure multiple default gateways
D. Use the Cisco Security MARS GUI or CLI to configure multiple default gateways

Answer: B

Question: 6

What are three ways to add devices to the Cisco Security MARS appliance? (Choose three.)

A. Import the devices from CiscoWorks
B. Import the devices from Cisco Security Manager
C. Load the devices from seed files
D. Use SNMP auto discovery
E. Use CDP to automatically discover the neighboring devices
F. Manually add the devices, one at a time

Answer: C, D, F

Question: 7

Which action enables the Cisco Security MARS appliance to ignore false-positive events by either dropping the events completely, or by just logging them to the database?

A. Creating system inspection rules using the drop operation
B. Creating drop rules
C. Inactivating the rules
D. Inactivating the events
E. Deleting the false-positive events from the Incidents page
F. Deleting the false-positive events from the Event Management page

Answer: B

Question: 8

Which three statements are true about Cisco Security MARS rules? (Choose three.)

A. There are three types of rules.
B. Rules can be saved as reports.
C. Rules can be deleted.
D. Rules trigger incidents.
E. Rules can be defined using a seed file.
F. Rules can be created using a query.

Answer: A,D,F

Question: 9

Which of the following alert actions can be transmitted to a user as notification that a Cisco Security MARS rule has fired, and that an incident has been logged? (Choose two.)

A. Distributed Threat Mitigation
B. Short Message Service
C. SNMP trap
D. XML notification
E. Syslog
F. OPSEC-LEA (clear and encrypted)

Answer: B, D