



## [Cisco 642-567](#)

**Exam Name:** *Advanced Security for Field Engineers*

**Q & A :** 65 Q&As

***Pdf Demo***

### **Quality and Value for the 642-567 Exam**

[Just4Exams Practice Exams](#) for Cisco Others 642-567 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

### **100% Guarantee to Pass Your 642-567 Exam**

If you do not pass the Others 642-567 exam on your first attempt using our Just4Exams **642-567 testing engine and pdf study guide**, we will give you a FULL REFUND of your purchasing fee.

### **Downloadable, Interactive 642-567 Testing engines and PDF Version**

Our Exam Preparation Material provides you everything you will need to take a [Others certification](#) examination. Details are researched and produced by [Cisco Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

#### **Free 642-567 Exams:**

***This is demo only, this pdf do not include the questions and answers picture***

Exam : Cisco 642-567

Title : Cisco(r) Advanced Security for Field Engineers

1. When configuring Cisco ACS users and groups, and the user configuration has an attribute configured differently from the same attribute in the group profile, what will the result be?

- A. The user setting will override the group setting.
- B. The group setting will be applied.
- C. The specific user cannot be placed into a group to avoid conflicts.
- D. A unique group must be configured and the user placed into that group.

Answer: A

2. What enables the MARS Appliance to profile network usage and detect statistically significant anomalous behavior from a computed

baseline?

- A. MARS Global Controller
- B. VMS
- C. Netflow
- D. CiscoWorks
- E. MARS custom parser

Answer: C

3. Which action enables the 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 events
- E. Deleting the false positive events from the Incidents > False Positives screen
- F. Deleting the false positive events from the Management > Event Management screen

Answer: B

4. Which of the following is a supported mitigation feature on the MARS Appliance?

- A. Generating and pushing configuration commands to Layer 3 devices
- B. Generating and pushing configuration commands to Layer 2 devices
- C. Automatically dropping all suspected traffic at the nearest firewall
- D. Automatically dropping all suspected traffic at the nearest IPS appliance

Answer: B

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

- A. Use the MARS GUI to enable a dynamic routing protocol.
- B. Use the MARS GUI to add a static route.
- C. Use the MARS GUI to configure multiple default gateways.
- D. Use the MARS CLI to enable a dynamic routing protocol.
- E. Use the MARS CLI to add a static route.
- F. Use the MARS CLI to configure multiple default gateways.

Answer: E

6. When restoring archived data to a MARS Appliance, which is the best practice to follow?

- A. Use HTTPS to protect the data transfer.
- B. Use secured FTP to protect the data transfer.
- C. Use "mode 5" restore from the MARS CLI to provide enhanced security during the data transfer.
- D. Use the Admin > System Maintenance > Data Archiving on the MARS GUI to perform restore operations online.
- E. To avoid problems, only restore to a same or higher-end MARS Appliance.

Answer: E

7. Which browser plug-in is required to view the charts and graphs on the MARS Appliance?

- A. Macromedia Flash Player
- B. Sun Microsystems Java
- C. Microsoft PowerPoint
- D. Adobe SVG Viewer

Answer: D

8. Which is a benefit of using the dollar variable (like \$TARGET01) when creating queries in MARS?

- A. The dollar variable enables multiple queries to reference the same common 5-tuples 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.

Answer: B

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

- A. After submitting the query, the MARS GUI screen will be locked up until the query completes.
- 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.
- E. You will be prompted to "Submit Inline" to run the query immediately.

Answer: D

10. What are three benefits in deploying MARS Appliances using the Global and Local Controllers' architecture? (Choose three.)

- A. A Global Controller can provide a summary of all Local Controllers information (network topologies, incidents, queries, and reports result).
- B. A Global Controller can provide a central point for creating rules and queries, which are applied to multiple Local Controllers simultaneously.
- C. The architecture provides redundancy in case one of the MARS Local Controllers failed within a zone.
- D. Users can seamlessly navigate to any Local Controllers from the Global Controller GUI.
- E. A Global Controller can correlate events from multiple Local Controllers to perform global sessionizations.

Answer: ABD

11. Which three statements are correct about the MARS Global Controller? (Choose three.)

- A. The Global Controller can correlate events from different Local Controllers into a common session.
- B. One Global Controller can support multiple Local Controllers.
- C. Each zone can have one Local Controller.
- D. All Local Controllers events are propagated to the Global Controller for correlations.
- E. The Global Controller and the Local Controllers can be running different MARS OS versions.
- F. Based on a selected Local Controller, incidents on the Global Controller can be viewed.

Answer: BCF

12. When adding a device to the MARS Appliance, what is the reporting IP address of the device?

- A. the source IP address that sends syslog information to the MARS Appliance
- B. the IP address MARS uses to access the device via SNMP
- C. the IP address MARS uses to access the device via Telnet or SSH
- D. the pre-NAT IP address of the device
- E. the highest loopback IP address configured on the Cisco reporting device

Answer: A

13. Which two of the following are required to enable MARS level 3 operations? (Choose two.)

- A. Global Controller
- B. vulnerability scanning
- C. Netflow
- D. SNMP community string
- E. username and password to log in to the device

Answer: DE

14. Regarding MARS Appliance rules, which three statements are correct? (Choose three.)

- A. There are three types of rules: System Inspection Rules, User Inspection Rules, and Drop 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: ADF

15. The MARS Appliance (running release 3.4.1) supports which protocol for data archiving and restoring?

- A. NFS
- B. TFTP
- C. FTP
- D. secured FTP

Answer: A

More [642-567 Braindumps](#) Information

#### Related 642-567 Exams

642-524	642-436	642-972	650-175	646-223
642-504	642-145	642-456	642-741	642-426

#### Other Cisco Exams

642-971	642-356	642-871	642-831	642-821
642-383	646-229	350-018-	350-023	642-655

640-460	642-383	642-731	650-180	646-230
646-563	642-373	646-363	642-975	646-656

		LAB	642-661	642-891
642-359	650-178	350-029	642-691	642-452
642-444	646-574	650-059		