

## 642-567 braindumps

### Cisco Others

#### 642-567: Advanced Security for Field Engineers

**Practice Exam:** 642-567 Exams

**Exam Number/Code:** 642-567

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

**Questions and Answers:** 65 Q&As

( [Others](#) )



"Advanced Security for Field Engineers", also known as 642-567 exam, is a Cisco certification. With the complete collection of exam questions, Just4Study has assembled to take you through 65 Q&As to your 642-567 exam preparation. In the 642-567 exam resources, you will cover every field and category in Cisco Certification helping to ready you for your successful Cisco Certification.

Exam : [642-567](#)

The exam questions cover the latest real test and with all the correct answer. we promise the Q&A for Cisco Others 642-567 (Advanced Security for Field Engineers) examination of original title complete coverage. 642-567 exam questions help you pass the exam.

#### **Just4Study 642-567 Feature:**

\* High quality - High quality and valued for the 642-567 Exam: 100% Guarantee to Pass Your 642-567 exam and get your Others certification.

\* Authoritative - Authoritative braindumps with complete details about 642-567 exam.

\* Cheaper - Our Just4Study products are cheaper than any other website. With our completed Others resources, you will minimize your **Cisco Others** cost and be ready to pass your 642-567 exam on Your First Try, 100% Money Back Guarantee included!

\* Free - Try free Others demo before you decide to buy it in <http://www.Just4Study.com>.

#### **Just4Study Guarantee:**

Just4Study provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if you do not pass the 642-567 exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### **Free 642-567 Demo Download**

Just4Study offers free demo for Others 642-567 exam (Advanced Security for Field Engineers). You can check out the interface, question quality and usability of our practice exams before you decide to buy it. We are the only one site can offer demo for almost all products.

The Questions & Answers cover the latest real test and with all the correct answer. we promise the Q&A for **Cisco Others 642-567** examination of original title complete coverage. 642-567 Questions & Answers help you pass the exam. Otherwise, we will give you a full refund.

**VUE/Prometric Code: 642-567**

Exam Name: Advanced Security for Field Engineers( Others )

Questions and Answers: 65 Q&A

[Cisco 642-567](#) Test belongs to one of the Others certified test, if needs to obtain the Others certificate, you also need to participate in other related test, the details you may visit the [Others](#) certified topic, in there, you will see all related Others certified subject of examination.

Just4Study professional provide Others 642-567 the newest Q&A, completely covers 642-567 test original topic. With our complete Others resources, you will minimize your Others cost and be ready to pass your 642-567 tests on Your First Try, 100% Money Back Guarantee included!

### **Just4Study Help You Pass Any IT Exam**

[Just4Study.com](#) offers incredible career enhancing opportunities. We are a team of IT professionals that focus on providing our customers with the most up to date material for any IT certification exam. This material is so effective that we Guarantee you will pass the exam or your money back.

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. 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

3. 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

4. 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

5. 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

6. 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

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. 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

9. 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

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. 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

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 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

14. 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

15. 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

### [642-567 Braindumps](#)

#### **Related 642-567 Exams**

[642-436](#) *Cisco Voice over IP (CVOICE)*

[642-145](#) *Implementing Cisco IOS Unified Communications Advanced*

[642-456](#) *Implementing Cisco Unified Communications Manager Part 2 (CIPT2 v6.0)*

[642-524](#) *Securing Networks with ASA Foundation*

[642-504](#) *Securing Networks with Cisco Routers and Switches*

[642-426](#) *Troubleshooting Unified Communications (TUC)*

[640-460](#) *IIUC Implementing Cisco IOS Unified Communications (IIUC)*

[642-383](#) *Cisco Express Foundation for Field Engineers*

[646-230](#) *Advanced Unified Communications AM*

646-656 *Wide Area Application Services for Account Managers*

646-223 *Unified Communications Express AM*

642-972 *Data Center Application Services Design*

642-974 *Data Center Networking Infrastructure Support Specialist*

646-563 *Advanced Security for Account Managers Exam*

646-363 *Cisco Express Foundation for Account Managers*

646-976 *Data Center Networking Sales Specialist*

642-971 *Data Center Networking Infrastructure Design Specialist*

642-373 *Cisco Express Foundation for Systems Engineers*

650-180 *SMBEN SMB Solutions for Engineers*

642-973 *Cisco Data Center Networking Infrastructure*

### **Other Cisco Exams**

642-445      640-816      646-204      640-801      350-024      642-973      351-001      642-871

646-671      642-242      642-425      646-202      642-972      351-018      642-873      642-181

642-545      646-362      642-355      642-055