

642-567 Others

Cisco Advanced Security for Field Engineers

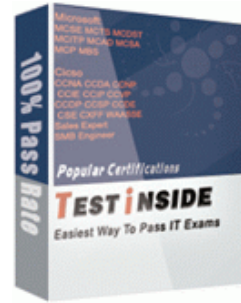
Practice Exam: 642-567 Exams

Exam Number/Code: 642-567

Exam Name: Advanced Security for Field Engineers

Questions and Answers: 65 Q&As

([Others](#))



Exam : [642-567](#)

"Advanced Security for Field Engineers", also known as 642-567 exam, is a Cisco certification. With the complete collection of questions and answers, TestInside 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.

Quality and Value for the 642-567 Exam TestInside Practice Exams for Cisco **Others** Certification 642-567 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

TestInside provide the professional Q&A.

1. We offer free update service for three month.

After you purchase our product, we will offer free update in time for three month.

2. High quality and Value for the 642-567 Exam.

642-567 simulation test questions, including the examination question and the answer, complete by our senior IT lecturers and the Others product experts, included the current newest 642-567 examination questions.

3. 100% Guarantee to Pass Your Others exam and get your Others Certification.

If you do not pass the Cisco Certification 642-567 exam (Advanced Security for Field Engineers) on your first attempt using our TestInside testing engine and pdf file, we will give you a FULL REFUND of your purchasing fee.

use TestInside 642-567 Q&A ensure you pass the exam at your first try.

TestInside 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!

[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.

TestInside Testing Engine Features

Comprehensive questions and answers about 642-567 exam

642-567 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

642-567 exam questions updated on regular basis

Same type as the certification exams, 642-567 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 642-567 exam demo before you decide to buy it in Test-Inside.com.

Note: This pdf demo do not include the question's picture.

Exam : Cisco 642-567

Title : Cisco(r) Advanced Security for Field Engineers

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

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 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

[More 642-567 Information](#)

Related 642-567 Exams

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

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

[642-972](#) *Data Center Application Services Design*

[650-175](#) *SMBAM SMB Specialization for Account Managers*

[646-223](#) *Unified Communications Express AM*

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

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

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

[642-741](#) *Implementing Cisco Unified Wireless Voice Networks*

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

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

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

[642-731](#) *Conducting Cisco Unified Wireless Site Survey*

[650-180](#) *SMBEN SMB Solutions for Engineers*

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

646-563 *Advanced Security for Account Managers Exam*

642-373 *Cisco Express Foundation for Systems Engineers*

646-363 *Cisco Express Foundation for Account Managers*

642-975 *Cisco Data Center Application Services Implementation*

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

Other Cisco Exams

642-524 350-024 640-821 646-393 642-112 642-511 642-052 642-541

350-040 642-274 650-251 642-067 642-566 640-863 646-363 642-591

642-979 650-173 642-545 642-552