

642-513 braindumps

Cisco CCSP

642-513: Securing Hosts Using Cisco Security Agent Exam (HIPS)

Practice Exam: 642-513 Exams

Exam Number/Code: 642-513

Exam Name: Securing Hosts Using Cisco Security Agent Exam (HIPS)

Questions and Answers: 69 Q&As

([CCSP](#))



Exam : [642-513](#)

"Securing Hosts Using Cisco Security Agent Exam (HIPS)", also known as 642-513 exam, is a Cisco certification. With the complete collection of exam questions, Just4Study has assembled to take you through 69 Q&As to your 642-513 exam preparation. In the 642-513 exam resources, you will cover every field and category in Cisco Certification helping to ready you for your successful Cisco Certification.

The exam questions cover the latest real test and with all the correct answer. we promise the Q&A for Cisco CCSP 642-513 (Securing Hosts Using Cisco Security Agent Exam (HIPS)) examination of original title complete coverage. 642-513 exam questions help you pass the exam.

Just4Study 642-513 Feature:

* High quality - High quality and valued for the 642-513 Exam: 100% Guarantee to Pass Your 642-513 exam and get your CCSP certification.

* Authoritative - Authoritative braindumps with complete details about 642-513 exam.

* Cheaper - Our Just4Study products are cheaper than any other website. With our completed CCSP resources, you will minimize your **Cisco CCSP** cost and be ready to pass your 642-513 exam on Your First Try, 100% Money Back Guarantee included!

* Free - Try free CCSP 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 642-513 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 642-513 Demo Download

Just4Study offers free demo for CCSP 642-513 exam (Securing Hosts Using Cisco Security Agent Exam (HIPS)). 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 CCSP 642-513** examination of original title complete coverage. 642-513 Questions & Answers help you pass the exam. Otherwise, we will give you a full refund.

VUE/Prometric Code: 642-513

Exam Name: Securing Hosts Using Cisco Security Agent Exam (HIPS)(CCSP)

Questions and Answers: 69 Q&A

[Cisco 642-513](#) Test belongs to one of the CCSP certified test, if needs to obtain the CCSP certificate, you also need to participate in other related test, the details you may visit the [CCSP](#) certified topic, in there, you will see all related CCSP certified subject of examination.

Just4Study professional provide CCSP 642-513 the newest Q&A, completely covers 642-513 test original topic. With our complete CCSP resources, you will minimize your CCSP cost and be ready to pass your 642-513 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 642-513

Title : Securing Hosts Using Cisco Security Agent Exam (HIPS)

1. Which one of the five phases of an attack attempts to become resident on a target?

- A. probe phase
- B. penetrate phase
- C. persist phase
- D. propagate phase
- E. paralyze phase

Answer: C

2. What is a benefit of putting hosts into groups?

- A. There is no need to configure rules.
- B. There is no need to configure rule modules.
- C. The administrator can deploy rules in test mode.
- D. The administrator does not have to deploy rules in test mode.

Answer: C

3. Which action do you take when you are ready to deploy your CSA configuration to systems?

- A. select
- B. clone
- C. deploy
- D. generate rules

Answer: D

4. What is the purpose of the Compare tool?

- A. to save data that has been configured
- B. to compare individual rules
- C. to compare individual rule modules
- D. to compare and merge configurations

Answer: D

5. Which three items make up rules? (Choose three.)

- A. variables
- B. applications
- C. application classes
- D. rule modules
- E. policies
- F. actions

Answer: ACF

6. What is the maximum number of characters that a policy name can contain?

- A. 24
- B. 32
- C. 48
- D. 64

Answer: D

7. Which information is logged for file access control?

- A. port and direction
- B. registry key
- C. process path
- D. PROGID/CLSID

Answer: C

8. If a Solaris or Windows system is not rebooted after CSA installation, which three rules are only enforced when new files are opened, new processes are invoked, or new socket connections are made? (Choose three.)

- A. COM component access rules
- B. network shield rules
- C. buffer overflow rules
- D. network access control rules
- E. file access control rules
- F. demand memory access rules

Answer: CDE

9. For which operating system is the network shield rule available?

- A. OS2
- B. Windows
- C. Linux
- D. Solaris

Answer: D

10. What is the purpose of the Audit Trail function?

- A. to generate a report listing events matching certain criteria, sorted by event severity
- B. to generate a report listing events matching certain criteria, sorted by group
- C. to generate a report showing detailed information for selected groups
- D. to display a detailed history of configuration changes

Answer: D

11. In which type of rules are network address sets used?

- A. COM component access control rules
- B. connection rate limit rules
- C. network access control rules
- D. file control rules
- E. file access control rules

Answer: C

12. When should you use preconfigured application classes for application deployment investigation?

- A. never
- B. always
- C. only for specific applications
- D. only when applications require detailed analysis

Answer: A

13. Which systems with specific operating systems are automatically placed into mandatory groups containing rules for that operating system? (Choose three.)

- A. OS2
- B. HPUX
- C. Solaris
- D. Mac OS
- E. Linux
- F. Windows

Answer: CEF

14. What information is logged for registry access control?

- A. port and direction
- B. registry key
- C. registry access events
- D. PROGID/CLSID

Answer: B

15. Which three of these does the buffer overflow rule detect on a UNIX operating system, based on the type of memory space involved? (Choose three.)

- A. location space
- B. stack space
- C. slot space
- D. data space
- E. heap space
- F. file space

Answer: BDE

16. Which action must be taken before a host can enforce rules when it has been moved to a new group?

- A. save
- B. generate rules
- C. deploy
- D. clone

Answer: B

17. What is the purpose of network access control rules?

- A. to control access to network services
- B. to control access to network addresses
- C. to control access to both network services and network addresses
- D. to control access to networks

Answer: C

18. Which protocol should never be disabled on the CSA MC?

- A. SSH
- B. Telnet
- C. IPSec
- D. SSL

Answer: D

19. Which of these is a reason for using groups to administer Agents?

- A. to link similar devices together
- B. to complete configuration changes on groups instead of hosts

- C. to complete the same configuration on like items
 - D. to apply the same policy to hosts with similar security requirements
- Answer: D

[642-513 Braindumps](#)

Related 642-513 Exams

642-515	<i>Securing Networks with ASA Advanced</i>
642-545	<i>Implementing Cisco Security Monitoring, Analysis and Response System</i>
642-542	<i>Cisco SAFE Implementation Exam</i>
642-552	<i>Securing Cisco Network Devices Exam</i>
642-513	<i>Securing Hosts Using Cisco Security Agent Exam (HIPS)</i>
642-502	<i>Securing Networks with Cisco Routers and Switches Exam (SNRS)</i>
642-503	<i>Securing Networks with Cisco Routers and Switches</i>
642-523	<i>Securing Networks with PIX and ASA</i>
642-522	<i>Securing Networks with PIX and ASA Exam (SNPA)</i>
642-521	<i>Cisco Secure PIX Firewall Advanced</i>
642-532	<i>Securing Networks Using Intrusion Prevention Systems Exam (IPS)</i>
642-551	<i>Securing Cisco Network Devices Exam (SND)</i>

Other Cisco Exams

640-821	642-523	642-551	642-321	646-588	642-054	640-822	650-180
642-811	642-241	642-521	640-460	646-228	646-967	642-891	642-821
642-564	640-811	642-504	642-426				