

Exam4Test 310-303 Exams

SUN Sun Certified Security Administrator for the Solaris 10 OS



Practice Exam: 310-303

Exam Number/Code: 310-303

Exam Name: Sun Certified Security Administrator for the Solaris 10 OS

Questions and Answers: 295 Q&As

Exam Description

Order : [310-303 Exam](#)

1. Exam4Test 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 310-303 Exam.

Exam4Test **Practice Exams** for 310-303 are written to the highest standards of technical accuracy, provided by our certified subject matter experts and published authors for development.

3. 100% Guarantee to Pass Your **SCSA10** exam and get your *SCSA10 Certification*.

We guarantee your success in the first attempt. If you do not pass the **SCSA10** "310-303" (Sun Certified Security Administrator for the Solaris 10 OS on your first attempt, send us the official result. We will give you a FULLY REFUND of your purchasing fee and send you another same value product for free.

4. Exam4Test SCSA10 310-303 Exam Downloadable.

Our PDF or Testing Engine Preparation Material of SCSA10 310-303 exam provides everything which you need to pass your exam. The SCSA10 Certification details are researched and produced by our Professional Certification Experts who are constantly using industry experience to produce precise, and logical. You may get "310-303 exam" questions from different websites or books, but logic is the key. Our Product will help you not only pass in the first Sun Certified Security Administrator for the Solaris 10 OS(SCSA10) exam try, but also save your valuable time.

Comprehensive questions with complete details about 310-303 exam.

310-303 exam questions accompanied by exhibits. Verified Answers Researched by Industry Experts and almost 100% correct.

Drag and Drop questions as experienced in the Real SCSA10 exam. 310-303 exam questions updated on regular basis.

Like actual SCSA10 Certification exams, 310-303 exam preparation is in multiple-choice questions (MCQs). Tested by many real SCSA10 exams before publishing.

Try free SCSA10 exam demo before you decide to buy it in <http://www.Exam4Test.com>

High quality and Valued for the 310-303 Exam: 100% Guarantee to Pass Your 310-303 exam and get your SCSA10 Certification. Come to <http://www.Exam4Test.com> The easiest and quickest way to get your SCSA10 Certification.

Exam4Test professional provides SCSA10 310-303 the newest Q&A, completely covers 310-303 test original topic. With our completed SCSA10 resources, you will minimize your SCSA10 cost and be ready to pass your 310-303 tes on Your First Try, 100% Money Back Guarantee included!

310-303 Exam Study Guide

310-303 exam is regarded as one of the most favourite [SCSA10 Certifications](#). Many IT professionals prefer to add 310-303 exam among their credentials. Exam4Test not only caters you all the information regarding the 310-303 exam but also provides you the excellent 310-303 study guide which makes the certification exam easy for you.

Exam4Test Engine Features

Comprehensive questions and answers about 310-303 exam

310-303 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

310-303 exam questions updated on regular basis

Same type as the certification exams, 310-303 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 310-303 exam demo before you decide to buy it in Exam4Test.com

Exam4Test Help You Pass Any IT Exam

[Exam4Test.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 : SUN 310-303

Title : Sun Certified Security Administrator for the Solaris 10 OS

1. Click the Exhibit button.

You maintain a minimized and hardened web server. The exhibit shows the current credentials that the web server runs with. You receive a complaint about the fact that a newly installed web-based application does not function. This application is based on a /bin/ksh cgi-bin script.

What setting prevents this cgi-bin program from working?

- A. The system might NOT have /bin/ksh installed.
- B. The server is NOT allowed to call the exec system call.
- C. The server should run with uid=0 to run cgi-bin scripts.
- D. Some of the libraries needed by /bin/ksh are NOT present in the webserver's chroot environment.

Answer: B

2. Which two tasks does the Key Distribution Center (KDC) perform? (Choose two.)

- A. issues service tickets
- B. authenticates services
- C. issues ticket-granting-tickets
- D. validates passwords sent in clear text
- E. provides private sessions to services

Answer: AC

3. After a recent audit, you have been requested to minimize an existing Solaris system which runs a third party database application. Which two should you do before starting to minimize the system? (Choose two.)

- A. Back up the system.
- B. Remove any unneeded patches.
- C. Install the SUNWmet metacluster.
- D. Remove any unneeded packages.

E. Confirm with the vendor of the database software that they support minimization.

Answer: AE

4. Which are two advantages of the Service Management Facility compared to the init.d startup scripts? (Choose two.)

- A. It restarts processes if they die.
- B. It handles service dependencies.
- C. It has methods to start and stop the service.
- D. It specifies what the system should do at each run level.

Answer: AB

5. You have been asked to implement defense in depth for network access to a system, where a web server will be running on an Internet-facing network interface. Which is NOT contributing to the defense in depth?

- A. running the web server in a zone
- B. using svcadm to disable unused services
- C. using IP Filter to limit which network ports can be accessed from the Internet
- D. using VLANs on a single network interface instead of using multiple network interfaces
- E. using TCP wrappers to limit from which system SSH be used to connect to the system

Answer: D

6. A new security related patch has been released for the Solaris OS. This patch needs to be applied to the system that functions as your web server. The web server is configured to run in a non-global zone. Can you just use patchadd to apply the patch to the global zone to update the web server zone?

- A. No, you need to shut down the web server zone first.
- B. Yes, patches will be automatically applied to all zones.
- C. No, you need to apply the patch to the web server zone separately.
- D. Yes, but you must make sure that the web server zone is booted first.

Answer: B

7. Within the context of file integrity, rules can be implemented to change the scope of the Basic Audit and Report Tool (BART) manifest.

Given the rule file:

```
/home/bert/docs *.og[dt]
```

```
CHECK all
```

```
IGNORE mtime
```

Which two statements are valid? (Choose two.)

- A. All files on the system will be checked.
- B. The last modification time of all checked files will not be checked.
- C. Key words such as CHECK and IGNORE can NOT be used in a rule file.
- D. Only files with extension .ogt and .ogd in the directory /home/bert/docs will be checked.
- E. All files on the system will be checked, except for files with extensions .ogt and .ogd in the directory /home/bert/docs.

Answer: BD

8. You decided it was worth maintaining an extremely paranoid policy when configuring your firewall rules. Therefore, you had your management approve the implementation of a security policy stance to deny all inbound connection requests to your corporate network. How is it possible that you still suffer from remote exploits that your adversaries are using to obtain interactive sessions inside your firewall?

- A. TCP splicing is easy to do.
- B. Internal software may be vulnerable.
- C. UDP vulnerabilities are well-known and exploited.
- D. ICMP hijacking attacks can still succeed through any firewall.

Answer: B

9. One of the operators of the mainframe group was moved to the UNIX group and tasked to activate and configure password history. For every user, the last 10 passwords should be remembered in the history. In what file is the size of the password history configured?

- A. /etc/shadow
- B. /etc/pam.conf
- C. /etc/default/passwd
- D. /etc/security/policy.conf

Answer: C

10. Solaris Auditing supports the selective logging of which two kinds of events? (Choose two.)

- A. file access by selected users
- B. access to selected files by all users
- C. selected users making outbound network connections
- D. password changes which do not meet the system password policy

Answer: AC

11. The company security policy now requires very detailed auditing of all actions. This includes capturing all executed commands together with their arguments and the environment variables.

After activating auditing on all Solaris 10 systems, the security auditor complains about having to check the audit trail on each individual host. He asks for a central place to capture all audit trails.

Using standard Solaris 10 security features, which is a solution to this problem?

- A. Configure auditd to send email with the events.
- B. Configure auditd to send the output using syslog to a central loghost.
- C. Configure auditd to store the audit trail using NFS on a central server.
- D. Configure auditd to store the audit trail using LDAP in a central directory.

Answer: C

12. You are configuring a new system to be used as an intranet web server. After you have installed the minimal amount of packages and patched the system, you added the appropriate web server packages (SUNWapch2r and SUNWapch2u). By default, the web server daemon will be started using UID webservd and the basic privilege set. To comply with the company's policy of least privilege, you need to minimize the privileges that the web server will have. What will you modify to specify the privileges that the web service will run with?

- A. the PRIV_DEFAULT setting in /etc/security/policy.conf
- B. the defaultpriv setting of webservd in /etc/user_attr
- C. the privileges property of the web service in the SMF repository
- D. the privs property of the web service in /etc/security/exec_attr

Answer: C

13. Which two commands are part of Sun Update Connection? (Choose two.)

- A. /usr/bin/pkgadm
- B. /usr/bin/keytool
- C. /usr/sbin/smpatch
- D. /usr/sbin/patchadd
- E. /usr/bin/updatesmanager

Answer: CE

14. A security administrator is required to validate the integrity of a set of operating system files on a number of Solaris systems. The administrator decides to use the Solaris Fingerprint Database to validate configuration and data files as well as binaries and libraries. What command, available by default in Solaris 10, will help the security administrator collect the necessary information that will be used with the Solaris Fingerprint Database?

- A. md5sum
- B. digest
- C. encrypt
- D. elfsign

E. cryptoadm

Answer: B

15. A security administrator has a requirement to deploy the Solaris Security Toolkit onto all Solaris servers in the department. In this environment, there are a variety of platforms and operating system versions deployed. Onto which two platforms and operating system combinations can the Solaris Security Toolkit be deployed in a supported configuration? (Choose two.)

- A. x86, Solaris 2.4
- B. x64, Solaris 9
- C. x86, Solaris 10
- D. SPARC, Solaris 2.6
- E. SPARC, Solaris 8

Answer: CE

16. You have been asked to grant the user ennovy, a member of the staff group, read and write access to the file /app/notes which has the following properties:

```
ls -l /app/notes
```

```
-rw-rw---- 1 root app 0 Jun 6 15:11 /app/notes
```

Which options will NOT grant the user the ability to read and write the file?

- A. usermod -G app ennovy
- B. setfacl -m user:ennovy:rw- /app/notes
- C. setfacl -m group:staff:rw- /app/notes
- D. usermod -K defaultpriv=basic,file_dac_read,file_dac_write ennovy

Answer: D

17. To harden a newly installed Solaris OS, an administrator is required to make sure that syslogd is configured to NOT accept messages from the network. Which supported method can be used to configure syslogd like this?

- A. Run svcadm disable -t svc:/network/system-log.
- B. Edit /etc/default/syslogd to set LOG_FROM_REMOTE=NO.
- C. Edit /etc/rc2.d/S74syslog to start syslogd with the -t option.
- D. Edit /lib/svc/method/system-log to set LOG_FROM_REMOTE=NO.

Answer: B

18. A security administrator creates a directory called prevoy with the following access control policy:

```
$ getfacl prevoy
```

```
# file: prevoy
```

```
# owner: secadm
```

```
# group: secadm
```

```
user::rwx group::r-x #effective:r-x
```

```
mask:r-x
```

```
other:r-x
```

```
default:user::r--
```

```
default:user:sysadm:rw-
```

```
default:group::r--
```

```
default:group:sysadm:rw-
```

```
default:mask:rwx
```

```
default:other:---
```

Into this directory, the security administrator creates a file called secrets. The ls command reports the following for the prevoy directory and secrets file:

```
$ ls -ld . secrets
```

```
drwxr-xr-x+ 2 secadm secadm 512 Jun 6 16:38 .
```

```
-r--r----+ 1 secadm secadm 0 Jun 6 16:38 secrets
```

Which two actions can be successfully taken by the sysadm role? (Choose two.)

- A. The sysadm role can read the secrets file.

- B. The sysadm role can write to the secrets file.
- C. The sysadm role can remove the secrets file.
- D. The sysadm role can create new files under the prevoy directory.
- E. The sysadm role can change the Access Control Lists of the prevoy directory.

Answer: AB

19. The /etc/default/passwd file contains a number of configuration parameters that can be used to constrain the character composition of user passwords. What is one of the dangers of having password composition too tightly constrained?

- A. Password complexity rules apply only to the English alphabet.
- B. The entropy of the resulting password strings will be very high.
- C. Duplication of encrypted user password strings is much more likely.
- D. Limited password value possibilities can simplify brute force attacks.
- E. Passwords are harder to compute when using many character classes.

Answer: D

20. Given:

```
jupiter:$md5,rounds=2006$2amXesSj5$kCF48vPsHDjIKNXeEw7V.:12210:::
```

What is the characteristic of this /etc/shadow entry?

- A. User jupiter uses the md5 hash, with salt 2006\$2amXesSj5\$, and with the encrypted password \$kCF48vPsHDjIKNXeEw7V.
- B. User jupiter uses the 2a hash, with 2006 iterations of the hash, with salt 2amXesSj5, and with the encrypted password kCF48vPsHDjIKNXeEw7V.
- C. User jupiter uses the md5 hash, with 2006 iterations of the hash, with salt 2amXesSj5, and with the encrypted password kCF48vPsHDjIKNXeEw7V.
- D. User jupiter uses the md5 hash, with 2006 iterations of the hash, with no salt, and with the encrypted password \$rQmXesSj5\$kCF48vPsHDjIKNXeEw7V.

Answer: C

[More 310-303 Information](#)

Related 310-303 Exams

[310-200](#) Sun Certified System Administrator for Solaris 10 OS.Part 1

[310-202](#) Sun Certified System Administrator for Solaris 10 OS.Part 2

[310-302](#) Sun Certified Network Administrator for Solaris 10 OS

[310-303](#) Sun Certified Security Administrator for the Solaris 10 OS

[310-301](#) Sun Certified Security Administrator

Other SUN Exams

[310-090](#) [310-131](#) [310-011](#) [310-092](#) [310-502](#) [310-879](#) [310-100](#) [310-880](#)

[310-220](#) [310-540](#) [310-301](#) [310-810](#) [310-015](#) [310-875](#) [310-877](#) [310-066](#)

[412-600](#) [310-630](#) [310-610](#) [310-055](#)