

QUESTIONS & ANSWERS

Kill your exam at first Attempt



SUN

310-303

Sun Certified Security Administrator for the Solaris 10 OS

<https://killexams.com/pass4sure/exam-detail/310-303>



QUESTION: 280

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: B, D

QUESTION: 281

Given:

```
jupiter:$md5,rounds=2006$2amXesSj5$$kCF48vfPsHDjlKNXeEw7V.: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 \$kCF48vfPsHDjlKNXeEw7V.
- B. User jupiter uses the 2a hash, with 2006 iterations of the hash, with salt 2amXesSj5, and with the encrypted password kCF48vfPsHDjlKNXeEw7V.
- C. User jupiter uses the md5 hash, with 2006 iterations of the hash, with salt 2amXesSj5, and with the encrypted password kCF48vfPsHDjlKNXeEw7V.
- D. User jupiter uses the md5 hash, with 2006 iterations of the hash, with no salt, and with the encrypted password \$rQmXesSj5\$\$kCF48vfPsHDjlKNXeEw7V.

Answer: C

QUESTION: 282

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

QUESTION: 283

Solaris 10 provides password history checking out of the box. Which name services currently support this feature?

- A. NIS
- B. NIS+
- C. Kerberos
- D. local files

Answer: D

QUESTION: 284

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

QUESTION: 285

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: C, E

QUESTION: 286

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 envovy`
- 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 envovy`

Answer: D

QUESTION: 287

To allow a legacy system to connect to one of your hosts, you are required to enable remote login (`rlogin`) connections. However, you wish to disable the ability for users to use `.rhosts` files to allow password-less logins. You have enabled `rlogin` connections by running the following command: `# svcadm enable network/login:rlogin`. Which file do you need to modify to disable the use of `.rhosts` files?

- A. `/etc/pam.conf`
- B. `/etc/default/login`
- C. `/etc/default/rlogin`
- D. `/etc/inet/inetd.conf`

Answer: A

QUESTION: 288

Click the Exhibit button. A system administrator needs to minimize a freshly installed Solaris system. After verifying that the correct metacluster is installed, the administrator tries to further

minimize the number of installed set-uid binaries. After inspection, the administrator finds a number of printing related binaries, reviewing the relevant contents of the /var/sadm/install/contents file. What is the correct command to remove these set-uid binaries in a supported way?

```
/usr/bin/cancel f none 4511 root lp 13188 5124
1146352661 SUNWpcu
/usr/bin/lp f none 4511 root lp 28148 12979 1146352662
SUNWpcu
/usr/bin/lpset f none 4511 root lp 12304 48630
1146352662 SUNWpcu
/usr/bin/lpstat f none 4511 root lp 27528 15650
1146352662 SUNWpcu
/usr/sbin/lpmove f none 4511 root lp 12336 52989
1146352663 SUNWpcu
```

- A. `pkgrm SUNWpcu`
- B. `rm /usr/bin/cancel /usr/bin/lp /usr/bin/lpset /usr/bin/lpstat /usr/bin/lpmove`
- C. `chmod u-s /usr/bin/cancel /usr/bin/lp /usr/bin/lpset /usr/bin/lpstat /usr/bin/lpmove`
- D. `chmod u-x /usr/bin/cancel /usr/bin/lp /usr/bin/lpset /usr/bin/lpstat /usr/bin/lpmove`

Answer: A

QUESTION: 289

Click the Task button.



Solaris contains a number of different tools for carrying out auditing, each focused on auditing a different type of activity.

Place each tool next to the type of activity it audits.

Type of Audit

place here

Audits file system changes on a system

place here

Audits user activity on a system

place here

Audits configuration changes on a system

Tools

Basic Audit Reporting Tool

Solaris Security Toolkit

Solaris Auditing

Answer:

Type of Audit

Basic Audit Reporting Tool

Audits file system changes on a system

Solaris Auditing

Audits user activity on a system

Solaris Security Toolkit

Audits configuration changes on a system

Tools

Basic Audit Reporting Tool

Solaris Security Toolkit

Solaris Auditing

QUESTION: 290

While attempting to restart the cron service on a Solaris 10 system from the secadm account, a security administrator receives the following error message:

```
secadm$ svcadm -v restart cron
```

```
svcadm: svc:/system/cron:default: Couldn't create "restarter_actions" property group (permission denied).
```

Which two actions will permit the secadm account to restart the cron service? (Choose two.)

- A. Assign the Cron Management rights profile to secadm.
- B. Assign the sys_admin privilege to the secadm account.
- C. Add the sys_user_compat privilege to the secadm account.
- D. Add the secadm account to the /etc/cron/cron.allow file.
- E. Assign the solaris.smf.manage.cron authorization to secadm.

Answer: A, E

QUESTION: 291

A company has produced several inhouse applications that have to deal with authentication using passwords. The Solaris systems have been reconfigured to use the password history checking option. What is the impact of this change for their applications?

- A. All applications automatically benefit from the new password history checking.
- B. Only privilege aware applications will benefit from the password history checking.
- C. Every application has to be changed to call the new functions for password history checking.
- D. Applications which use the PAM framework will automatically use password history checking.

Answer: D

QUESTION: 292

Which item in the list would be specifically required for a VPN compared to a mode without encryption?

- A. Authentication Header (AH)
- B. Internet Key Exchange (IKE)
- C. Encapsulating Security Payload (ESP)
- D. Streams Control Transmission Protocol (SCTP)

Answer: C

QUESTION: 293

You have been asked to let your manager's children run their homework assignments on one of the servers you administer. You have been promised that it will not impact the overall performance of the server, but you aren't sure, so you want to track how many resources they use. After you have created a new user called kids and assigned a new project called homework to the user, what do you need to do to gather the resource usage information?

- A. Enable Solaris Auditing for the kids user.
- B. Use the acctadm command to enable extended accounting for tasks.
- C. Use the poolcfg command to assign the homework project to a resource pool.
- D. Use the rctladm command to enable the syslog action for the homework project.

Answer: B

QUESTION: 294

A security administrator has created these "Restricted Commands" rights profiles in the /etc/security/exec_attr file that will be assigned to a number of application developers:

```
$      grep      "^Restricted      Commands"      /etc/security/exec_attr      Restricted
```

Commands:solaris:cmd:::/my/bin/progA:uid=yadm;gid=yadm	Restricted
Commands:solaris:cmd:::/my/bin/progB:uid=vadm;gid=vadm	Restricted
Commands:solaris:cmd:::/my/bin/progC:uid=oamd;gid=aadm	Restricted
Commands:solaris:cmd:::/my/bin/progD:uid=nadm;gid=badm	Restricted
Commands:solaris:cmd:::/my/bin/progD:uid=nadm;gid=cadm	Restricted
Commands:solaris:cmd:::/my/bin/progD:uid=eadm;gid=eadm	Restricted
Commands:solaris:cmd:::/my/bin/progD:	

As what UID and GID will the command /my/bin/progD run when the command is executed as followed by an application developer who has been assigned the "Restricted Commands" rights profile?

- A. UID nadm and GID badm
- B. UID nadm and GID cadm
- C. UID eadm and GID eadm
- D. UID and GID of the application developer

Answer: A

QUESTION: 295

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

For More exams visit <https://killexams.com/vendors-exam-list>



Kill your exam at First Attempt....Guaranteed!