Oracle

1Z0-881

Oracle Solaris 10 Security Administrator(R) Certified Expert

QUESTION: 280
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: 281
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: 282
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: 283
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/updatemanager

Answer: C,E

QUESTION: 284
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

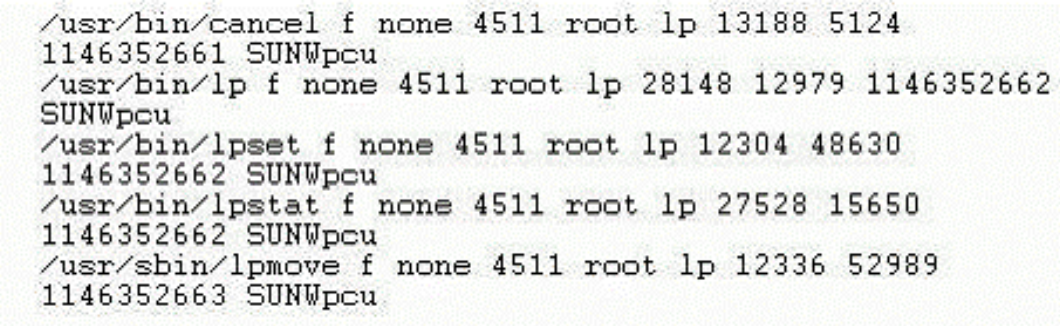
Answer: D

QUESTION: 285
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: 286
Click the Exhibit button.

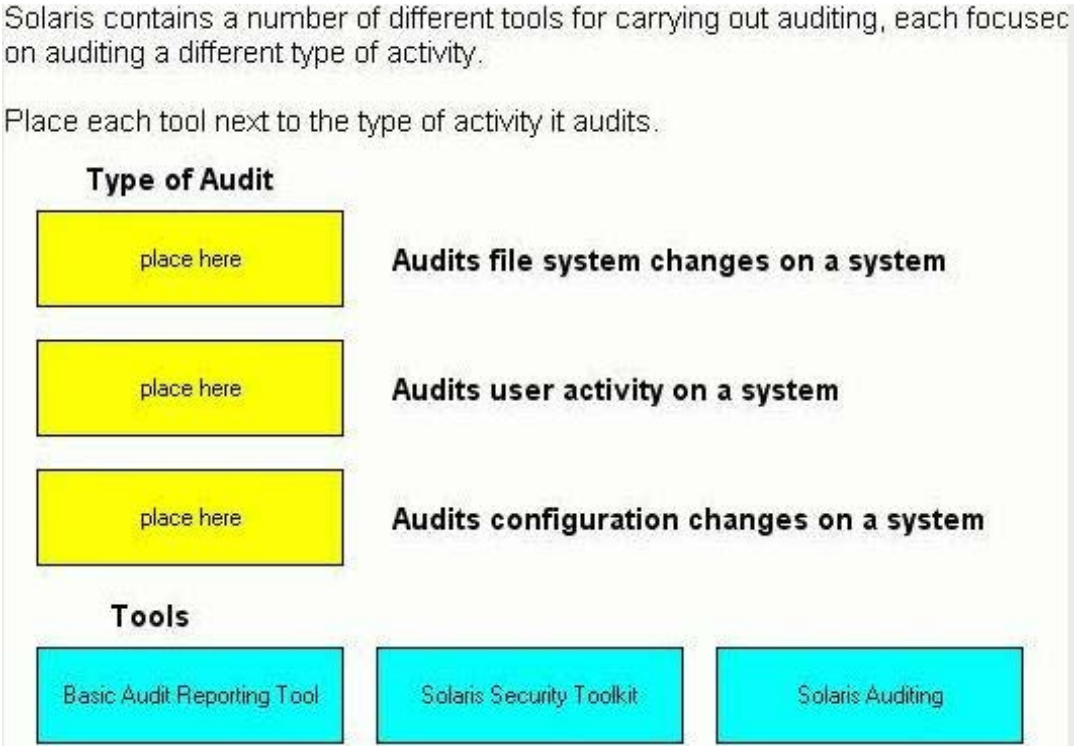


A system administrator needs to minimize a freshly installed Solaris system. After verifying that the correct metacluster is installed, the administrator tries to further minimize the number of installed set-uid binaries. After inspection, the administrator finds a number of printing related binaries, 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?

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

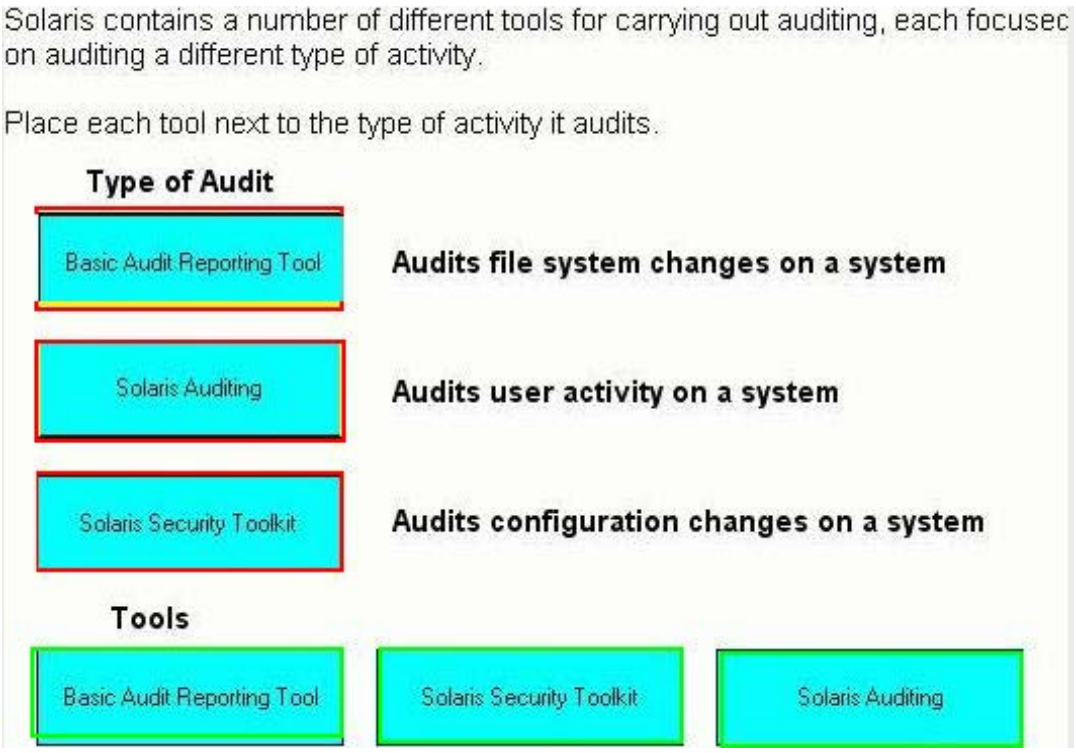
Answer: A

QUESTION: 287
DRAG DROP
Click the Task button.



Drag and drop question. Drag the items to the proper locations.

Answer:



QUESTION: 288
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_suser_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: 289
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: 290
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: 291
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: 292
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: 293
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 webserverd 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

Download Full Version From https://www.certkillers.net

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