Administration of Symantec Data Loss Prevention 12

1. A DLP administrator needs to forward data loss incidents to the company's Security Information and Event Management (SIEM) system. Which response rule action provides the administrator with the ability to accomplish this task?

A. All: Send Email Notification

B. All: Set Attribute

C. All: Log to a Syslog Server

D. All: Add Note

Answer(s): C

---

2. An administrator is checking System Overview and all of the detection servers are showing as 'unknown'. The Vontu services are up and running on the detection servers. Thousands of .IDC files are building up in the Incidents directory on the detection servers. There is good network connectivity between the detection servers and the Enforce server when testing with the telnet command. How can the administrator bring the detection servers to a running state in the Enforce UI?

A. restart the Vontu Monitor Service on all of the detection servers affected

B. ensure the Vontu Monitor Controller service is running on the Enforce server

C. delete all of the .BAD files in the incidents folder on the Enforce server

D. ensure port 8300 is configured as open on the firewall

Answer(s): B

---

3. You are responsible for administering the Storage Foundation for Oracle server. You plan to clone a database using Database FlashSnap. When you run the dbed_vmchecksnap command you get an error "SFORA dbed_vmchecksnap ERROR V-81-5677 Could not find a mandatory, primary and valid archive destination for database PROD." You want to resolve this error.

A. Empty the full mandatory location and make free space available for the Oracle database.

B. Change the default archive location.

C. Define the location of the archive logs in the UNC format.

D. Set the valid archive destination.

Answer(s): D

---

4. Which product can replace a confidential document residing on a share with a marker file explaining why the document was removed?

A. Network Discover

B. Mobile Prevent

C. Network Protect

D. Endpoint Discover

Answer(s): C

---

5. A DLP administrator is attempting to use Encryption Insight to detect confidential information in encrypted files but has been unsuccessful. It is determined that the process was unable to retrieve the appropriate PGP key because the user key was using the incorrect encryption mode.

A. Client Server Key Mode

B. Client Key Mode

C. Guarded Key Mode

D. Server Key Mode

Answer(s): D

---

6. An administrator running a company's first Discover scan needs to minimize network load. The duration of the scan is unimportant. Which method should the administrator use to run the Discover scan?

A. ignore larger than

B. throttling

C. ignore smaller than

D. date last accessed

Answer(s): B

---

7. A Network Monitor is showing under System Overview as 'Running Selected'. The corresponding detection server events indicate that packet capture and filereader are crashing.

A. the Enforce server and detection server are running different versions

B. the detection server is missing the server side certificate

C. the minimum required amount of available free space has been used

D. the license has expired for this detection server

Answer(s): C

---

8. Which file is required to decrypt the edpa_ext0.log using the Endpoint Agent logdump utility?

A. ks.ead

B. is.ead

C. cg.ead

D. dcs.ead

Answer(s): A

---

9. Which action is available for use in Smart Response rules and Automated Response rules?

A. modify SMTP message

B. post log to a syslog server

C. block email message

D. limit incident data retention

Answer(s): B

---

10. You are working on a Storage Foundation 5.0 server named Srv1 that has a disk group named vol1. You install another Storage Foundation 5.0 server named Srv2. You want to successfully move the disk group from Srv1 to Srv2. To initiate the movement, you stop all volumes in the disk group, and deport and move all disks to Srv2.

A. Create a new disk group.

B. Format the disk group.

C. Start the volumes in the disk group.

D. Recognize the disks using VxVM.

Answer(s): D

---

11. A user is unable to log in as sysadmin. The Data Loss Prevention system is configured to use Active Directory authentication. The user is a member of two roles: sysadmin and remediator.

A. sysadmin\username

B. username\sysadmin

C. sysadmin\username@domain

D. domain\username

Answer(s): A

---

12. Which detection server requires two physical network interface cards?

A. Network Discover

B. Network Protect

C. Network Monitor

D. Endpoint Discover

Answer(s): A

---

13. You place six physical disks under Volume Manager control to create 10GB of volume. You want to use this volume as an archive directory. You need to create a volume that will store three copies of the archived data. Which command will you use to create a volume with three plexes?

A. vxassist make archivevol 10g layout=stripe-mirror ncolumn=3

B. vxassist make archivevol 10g layout=stripe-mirror nmirror=3

C. vxassist make archivevol 30g layout=stripe-mirror nmirror=3

D. vxassist make archivevol 30g layout=stripe-mirror ncolumn=3

Answer(s): B

---

14. After installing Veritas Volume Manager for your large number of volumes, you will configure the volumes as per your requirement. But you find the performance is very slow. You need to reconfigure the volumes to achieve significant improvement in performance when there are multiple I/O streams.

A. Use Mirroring and Striping

B. Use Mirroring

C. Use RAID-5

D. Use Striping

Answer(s): B

---

15. A Network Monitor server has been installed and the networking components configured accordingly. The server is receiving traffic, but fails to detect incidents. Running Wireshark indicates that the desired traffic is reaching the detection server.

A. The mirrored port is sending corrupted packets.

B. The configuration is set to process GET requests.

C. The wrong interface is selected in the configuration.

D. The communication to the database server is interrupted.

Answer(s): A

---

16. You are the administrator of Veritas Volume Manager in Veritas Storage Foundation environment. You want to remove a disk from a disk group. You execute the command vxdg -g dg01rmdisk d001. After executing the command, you are prompted with the error "VxVM vxdg ERROR V-5-552 disk diskname is used by one or more subdisks." You want to ensure you are able to remove the disk from the disk group.

A. Use -t option with vxdg command

B. Use -n option with vxdg command

C. Use -o option with vxdg command

D. Use -k option with vxdg command

Answer(s): D

---

17. A DLP administrator needs to inspect HTTP traffic using a Network Monitor, including data pushed up to the web and data pulled down from the web.

A. L7.processGets=true, PacketCapture.DISCARD_HTTP_GET=false, L7.minSizeofGetURL=10

B. L7.processGets=false, PacketCapture.DISCARD_HTTP_GET=true, L7.minSizeofGetURL=1000

C. L7.processGets=true, PacketCapture.DISCARD_HTTP_GET=true, L7.minSizeofGetURL=100

D. L7.processGets=false, PacketCapture.DISCARD_HTTP_GET=false, L7.minSizeofGetURL=10

Answer(s): A

---

18. You need to provide storage space for database application, including permanent data, temporary space, and activity log data. You need to ensure that the storage space that you provide offers data protection against disk failures. Which storage techniques will you use? (Each correct answer presents part of the solution. Select two.)

A. RAID-0

B. Concatenated

C. RAID-5

D. RAID-1

E. RAID-1+0

Answer(s): C,D

---

19. When working on Storage Foundation 5.0 from Storage Foundation Management Server 1.0, you get an error "Could not connect to central server. Central server may not be running." Given the following steps:

A. 3,4,6,2,1,5

B. 3,1,4,2,6,5

C. 4,2,5,3,2,6

D. 5,4,1,2,6,3

Answer(s): B

---

20. You have installed all the features for Storage Foundation for DB2. On the VxFS file system, you execute a command /opt/VRTS/bin/qiomkfile -s 500m /db01/dbfile.

A. The command will create a concurrent I/O capable file.

B. The command will terminate without providing any result.

C. The command will resize a Quick I/O file to 500 MB.

D. The command will create a 500 MB Quick I/O capable file.

Answer(s): D