Administration of Symantec™ Data Center Security: Server Advanced 6.0 Sample Exam

Contents

Sample Questions

1. Which method is a Symantec recommended policy deployment method?

    a. Incremental Rollout
    b. Silent Install
    c. Push Mode Deployment
    d. LiveUpdate

2. The default Windows BaseLine Detection Policy contains a section called “Monitor System-Critical Files”

    Which files are included in the policy?

    a. Core System Files
    b. Security Database Files
    c. Core System Configuration Files
    d. Group Policy Files

3. The log files show that the management server is experiencing event-posting delays.

    Which two reasons can cause the delay? (Select two.)

    a. trivial events are uploaded in bulk
    b. too many events are being generated on the endpoints
    c. a user is logged into a protected system
    d. the database is overtaxed
    e. an alert or warning needs to be processed

4. Where is the default output found when an administrator initiates a Collect Agent Info from the management console?

    a. on the agent in the bulk log folder
    b. in the logfiles directory on the management server
    c. in the Symantec MySupport portal
    d. on the agent in the install directory

5. Which two actions can be performed on the Admin Page? (Select two.)

    a. view configurations applied to agents
    b. create roles and grant access to assets based on those roles
    c. configure Active Directory servers
    d. export report results to a file
    e. copy and delete policies

6. Which information can be collected by deploying the SDCSS_Agent_Status detection policy on a Windows agent?

    a. Data Center Security Server Registry settings on the agent
    b. details of the IDS service on the agent being stopped
    c. a list of users who have selected the Policy Override option on the agent
    d. the current status of the IPS service on the agent

7. Which statement accurately describes the Global_Watch_Policy feature?

    a. The Global_Watch_Policy can be applied across all agent platforms.
    b. The Global_Watch_Policy is applied to the management server to monitor Alert text files.
    c. The Global_Watch_Policy can be deployed to monitor all system events.
    d. The Global_Watch_Policy is deployed by default when the IDS agent is installed.

8. Which two elements describe, at a high level, how Symantec Data Center Security: Server Advanced protects the enterprise?

    a. real-time file integrity monitoring and patch upgrades
    b. host intrusion detection and host intrusion prevention
    c. configuration detection and network monitoring
    d. hands-on user control and authentication services

9. Which action should an administrator take to maximize performance of the management console?

    a. increase physical memory of the management server
    b. increase the disk space of the management console
    c. increase the database capacity
    d. increase the management console's heap space

10. When is the security tag removed from a malware infected guest virtual machine (VM)?

    a. after the clean completion of entire guest VM scan
    b. as soon as the NSX security policy is applied
    c. after the guest VM is moved to a security tag group
    d. as soon as the malware protection policy is applied

11. For which operating system does Symantec Data Center Security: Server Advanced include UNIX prevention policies?

    a. HP-UX 11i
    b. Solaris 11
    c. VMWare ESX 4.1
    d. Ubuntu 9.04

12. Which two services should be verified on the database server to enable the management server to connect to the database? (Select two.)

    a. SQL Server (*instancename*)
    b. Symantec Data Center Security Server Manager
    c. OracleService *instancename*
    d. SQL Server Browser

13. Which field in the Event Details confirms whether an action is allowed or denied?

    a. Agent State
    b. Disposition
    c. Operation
    d. Agent Type

14. Which two statements are accurate for real-time and bulk logging? (Select two.)

    a. use real-time logging for actionable events and bulk logging for non-critical ones
    b. real-time logging can dramatically reduce network load while providing capture of extensive, fine-grained detailed event data
    c. bulk logging mechanism can dramatically reduce network load while providing capture of extensive, fine-grained detailed event data
    d. bulk logging is needed for immediate display of events on the management console
    e. use real-time logging for efficient archival storage of all logged events

15. Which statement is accurate when describing real-time file monitoring?

    a. When enabled, real-time file monitoring is applied to all agents.
    b. When real-time file monitoring is enabled, the polling interval is shortened by default.
    c. Real-time file monitoring is performed by user-mode drivers.
    d. The real-time file monitoring polling interval is configured in the global default settings.

16. Which sandbox are programs that access files remotely confined to by default?

    a. Basic sandbox
    b. Read-only sandbox
    c. Fully-Open sandbox
    d. Hardened sandbox

17. Which two mechanisms can be used to send a notification when configuring an alert? (Select two.)

    a. SNMP
    b. SYSLOG
    c. SMTP
    d. HTTPS
    e. ICMP

18. Which two security management requirements are satisfied by appropriate implementation of Symantec Data Center Security: Server Advanced policies? (Select two.)

    a. scan systems and report on their compliance to a required standard
    b. prevent unauthorized access to a system using network based rules
    c. detect any changes to confidential data
    d. encrypt confidential data before allowing outward transmission from a system
    e. perform network discovery and asset management

19. Which two logon authentication methods are available for accessing the management console? (Select two.)

    a. SAML
    b. Pluggable Authentication Module
    c. Active Directory
    d. RADIUS
    e. Local Authentication

20. Which two event categories are used to verify the update applied successfully after deploying a Detection policy to a group of assets? (Select two.)

    a. Management
    b. Detection
    c. Analysis
    d. Audit
    e. Profile

Answers

1-a, 2-a, 3-b&d, 4-b, 5-b&c, 6-a, 7-b, 8-b, 9-d, 10-a, 11-c, 12-a&d, 13-b, 14-a&c, 15-c, 16-d, 17-a&c, 18-b&c, 19-c&e, 20-a&d

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com