# Testpassport考試指南

品　　質　　更　　高　　服　　務　　更　　好

一年免費更新服務

http://www.testpassport.net

**Exam** : **251-311**

**Title** : Administration of Symantec Endpoint Protection 11.0 for Windows

**Version** : DEMO

1. The Symantec Endpoint Protection Manager supports the use of which database solutions? (Choose two.)
A.Microsoft SQL Server 2000
B.MySQL Server 2005
C.Microsoft SQL Server 2005
D.Oracle Database 11g
E.Oracle Database 9i
ANSWER: AC

2. In the Symantec Endpoint Protection Manager console, where do you modify replication?
A.Admim > Servers > Server Properties > Directory Servers
B.Admin > Servers > Local Site > Replication Partner
C.Policies > Management Server Lists > Replication
D.Admin > Servers > Database > Tasks
ANSWER: B

3. What are the three configurable actions in TruScan Proactive Threat Scan? (Choose three.)
A.log suspect process only
B.set a public SNMP trap
C.quarantine suspect process
D.terminate the suspect process
E.generate dump of system state
F.suspend the suspect process
ANSWER: ACD

4. A computer is configured in Mixed Control mode. The administrator creates and applies a firewall policy to the computer that has a rule that allows FTP traffic above the blue line and another rule that blocks LDAP traffic below the blue line. On the computer, local rules are created to allow LDAP traffic and block FTP.
Which traffic flow behavior should be expected on the local computer?
A.Both FTP and LDAP traffic are allowed.
B.Both FTP and LDAP traffic are blocked.
C.FTP is blocked and LDAP is allowed.
D.FTP is allowed and LDAP is blocked.
ANSWER: A

5. What is one reason for disabling learned applications?
A.Learned applications can often expose usernames and passwords.
B.Learned applications require promiscuous mode.
C.Learned applications are often legitimate programs.
D.Learned applications are illegal in some countries.
ANSWER: D

6. An administrator believes that client computers are running different software versions of Symantec

Endpoint Protection.
Which report type shows which client computers are running different software versions?
A.Application and Device Control Report
B.System Report
C.Compliance Report
D.Computer Status Report
ANSWER: D

7. THE DISCLOSURE TO YOU OF THIS EXAMINATION ("THE EXAM") AND ANY ACCOMPANYING EXAMINATION MATERIALS AND ANY DERIVATIVES THEREOF (COLLECTIVELY REFERRED TO AS THE "EXAM MATERIALS") IS SUBJECT TO THE TERMS AND CONDITIONS OF THE SYMANTEC CORPORATION CONFIDENTIALITY AGREEMENT PROVIDED HEREIN. BY CLICKING ON THE "START" BUTTON IN RESPONSE TO THE ACCEPTANCE QUERY, OR BY OTHERWISE TAKING THE EXAMINATION, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. BY CLICKING ON THE "EXIT" BUTTON, YOU CHOOSE NOT TO AGREE AND WILL BE LET OUT OF THE EXAM.
IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS.
SYMANTEC CORPORATION CONFIDENTIALITY AGREEMENT
This is an agreement ("Agreement") between You and Symantec Corporation that sets forth the terms and conditions of your use and disclosure of the Exam Materials.
You hereby understand, acknowledge, and agree:
1.That Symantec Corporation spends substantial sums of time and money in developing and administering its Exam Materials and labs and carefully guards their integrity and confidentiality;
2.That the questions and answers of the Exam are the exclusive and confidential property of Symantec Corporation and are protected by Symantec Corporation's intellectual property rights;
3.That You may not disclose the Exam questions or answers or discuss any of the content of the Exam Materials with any person, without prior written approval of Symantec Corporation;
4.Not to remove from the examination room any Exam Materials of any kind provided to You or any other material related to the Exam, including, without limitation, any notes or calculations;
5.Not to copy or attempt to make copies (written, photocopied, or otherwise) of any Exam Material, including, without limitation, any exam questions or answers;
6.Not to sell, license, distribute, give away, or obtain from any other source other Symantec Corporation the Exam materials, questions or answers.
You hereby acknowledge and agree that violation of any of these provisions will cause irreparable harm to Symantec Corporation for which monetary remedies may be inadequate, and that Symantec Corporation shall be entitled, without waiving any other rights or remedies, to take all appropriate actions to remedy or prevent such disclosure or misuse, including obtaining an immediate injunction. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable by You. This Agreement may be modified only by a writing signed by both parties. This Agreement shall be construed in accordance with the laws of the State of California, without giving effect to any choice of law rule. This Agreement represents the entire Agreement of the parties hereto pertaining to the subject matter of this Agreement, and supersedes any and all prior oral discussions and/or written correspondence or agreements between the parties with respect thereto.
If you ACCEPT the terms and conditions of this Agreement, click 'Yes, I agree.', and begin this exam. If

you DO NOT ACCEPT this Agreement, you must click 'No, I do not agree.', and will not be able to proceed with this exam.
ANSWER:

8. THE DISCLOSURE TO YOU OF THIS EXAMINATION ("THE EXAM") AND ANY ACCOMPANYING EXAMINATION MATERIALS AND ANY DERIVATIVES THEREOF (COLLECTIVELY REFERRED TO AS THE "EXAM MATERIALS") IS SUBJECT TO THE TERMS AND CONDITIONS OF THE SYMANTEC CORPORATION CONFIDENTIALITY AGREEMENT PROVIDED HEREIN. BY CLICKING ON THE "START" BUTTON IN RESPONSE TO THE ACCEPTANCE QUERY, OR BY OTHERWISE TAKING THE EXAMINATION, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. BY CLICKING ON THE "EXIT" BUTTON, YOU CHOOSE NOT TO AGREE AND WILL BE LET OUT OF THE EXAM.
IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS.
SYMANTEC CORPORATION CONFIDENTIALITY AGREEMENT
This is an agreement ("Agreement") between You and Symantec Corporation that sets forth the terms and conditions of your use and disclosure of the Exam Materials.
You hereby understand, acknowledge, and agree:
1.That Symantec Corporation spends substantial sums of time and money in developing and administering its Exam Materials and labs and carefully guards their integrity and confidentiality;
2.That the questions and answers of the Exam are the exclusive and confidential property of Symantec Corporation and are protected by Symantec Corporation's intellectual property rights;
3.That You may not disclose the Exam questions or answers or discuss any of the content of the Exam Materials with any person, without prior written approval of Symantec Corporation;
4.Not to remove from the examination room any Exam Materials of any kind provided to You or any other material related to the Exam, including, without limitation, any notes or calculations;
5.Not to copy or attempt to make copies (written, photocopied, or otherwise) of any Exam Material, including, without limitation, any exam questions or answers;
6.Not to sell, license, distribute, give away, or obtain from any other source other Symantec Corporation the Exam materials, questions or answers.
You hereby acknowledge and agree that violation of any of these provisions will cause irreparable harm to Symantec Corporation for which monetary remedies may be inadequate, and that Symantec Corporation shall be entitled, without waiving any other rights or remedies, to take all appropriate actions to remedy or prevent such disclosure or misuse, including obtaining an immediate injunction. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable by You. This Agreement may be modified only by a writing signed by both parties. This Agreement shall be construed in accordance with the laws of the State of California, without giving effect to any choice of law rule. This Agreement represents the entire Agreement of the parties hereto pertaining to the subject matter of this Agreement, and supersedes any and all prior oral discussions and/or written correspondence or agreements between the parties with respect thereto.
If you ACCEPT the terms and conditions of this Agreement, click 'Yes, I agree.', and begin this exam. If you DO NOT ACCEPT this Agreement, you must click 'No, I do not agree.', and will not be able to proceed with this exam.
ANSWER:

9. What controls access from one network segment to another?
A.hub
B.MTA
C.sensor
D.firewall
ANSWER: D

10. Which label is given to a program or algorithm that replicates itself over a computer network and usually performs malicious actions?
A.virus
B.zero-day exploit
C.spam
D.worm
ANSWER: D

11. Which five components are incorporated in Symantec Endpoint Protection 11.0? (Choose five.)
A.antispam
B.application and device control
C.full disk encryption
D.host integrity
E.antivirus
F.antispyware
G.content filtering
H.intrusion prevention
I.client firewall
J.asset management
ANSWER: BEFHI

12. Which two statements are true about Symantec Endpoint Protection TruScan Proactive Threat Scan? (Choose two.)
A.It inspects encrypted network traffic.
B.It evaluates process behavior.
C.It uses malicious code detection signatures.
D.It blocks attackers' IP addresses.
E.It detects unknown threats.
ANSWER: BE

13. Which Network Threat Protection technologies of the Symantec Endpoint Protection client provide the primary protection layers against network attacks?
A.Proactive Threat Protection and Network Access Control
B.Proactive Threat Protection and Client Firewall
C.Intrusion Prevention and Client Firewall
D.Client Firewall and Network Access Control
ANSWER: C

14. Lifeline Supply Company wants to reduce or eliminate the HelpDesk calls they receive due to end users modifying, moving, or deleting configuration files.
Which component of Symantec Endpoint Protection will allow the IT administrator to prevent users from altering configuration files?
A.TruScan Proactive Threat Scan
B.Device Control
C.Application Control
D.Host Integrity
ANSWER: C

15. Lifeline Supply Company found during a recent audit that the current security solution for their desktops and servers missed several rootkits within their environment. These rootkits have compromised several company computers.
Which protection technology in Symantec Endpoint Protection could remediate these rootkits?
A.Host Integrity
B.Antivirus and Antispyware Protection
C.Network Threat Protection
D.Application and Device Control
ANSWER: B

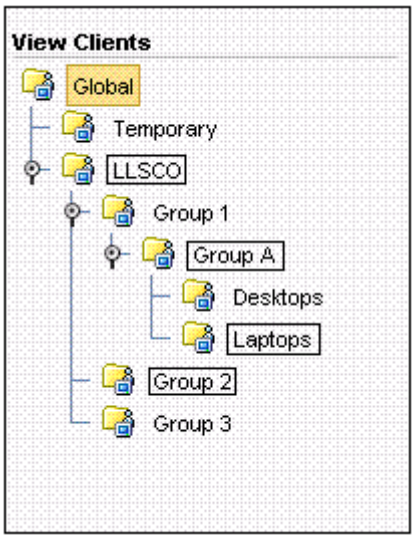
16. Which page is used to create login accounts to the Symantec Endpoint Protection Manager console?
A.Policies
B.Home
C.Admin
D.Clients
ANSWER: A

17. A company has a large sales force who travel with laptops. They want to block USB access on the laptops when they are disconnected from the corporate network.
Which two things are required to achieve this? (Choose two.)
A.multiple sites
B.multiple locations
C.firewall policy
D.device control policy
E.host integrity policy
ANSWER: BD

18. Where can you edit a non-shared policy?
A.Clients
B.Monitors
C.Home
D.Admin

ANSWER: A

19. Refer to the exhibit.
Inheritance is turned on for groups LLSCO, Group A, Laptops, and Group 2 (outlined).
Without turning inheritance off, which top level group must be modified to affect users in the Laptop group?
A.Desktops
B.Laptops
C.Group 1
D.Group A




ANSWER: C

20. The administrators at Lifeline Supply Company have a manufacturing facility that runs three shifts. Employees at the facility must share computers. The administrators want the ability to apply different policies/configurations for each shift.
How can the administrator configure the environment to allow policies to be applied to each shift? (Choose two.)
A.create one group for all computers in the facility
B.create one group for all users in the facility
C.create one group for all computers on each shift
D.create one group for all users on each shift
E.switch the clients to computer mode
F.switch the clients to user mode
ANSWER: DF