# IT 认证电子书

半年免费升级服务

质 量 更 高 服 务 更 好

**Exam**    :    **ST0-029**

**Title**    :    Symantec Endpoint
Protection 11 (STS)

**Version**    :    Demo

1. Which Symantec Network Access Control method supports basic and transparent mode for 802.1x?

A. Gateway Enforcer

B. Self Enforcement

C. DHCP Enforcer

D. LAN Enforcer

**Answer:** D


2. When using the Push Deployment wizadr, which two methods can you use to identify the target

machines to which you want to install the Symantec Endpoint Protection client? (Select two.)

A. browse through Windows Networking

B. import a file containing IP addresses

C. specify a UNC path

D. import a file containing MAC addresses

E. import hostnames from an LDAP server

**Answer:** AC


3. From where does the Migration and Deployment wizadr collect settings?

A. configuration file

B. Symantec Client Firewall Administrator

C. Symantec AntiVirus server

D. Active Directory server

**Answer:** C


4. In which group can you NOT create new subgroups?

A. Global

B. Subgroup

C. Temporary

D. Administrator-created

**Answer:** C

5. Which four events trigger an Auto-Protect scan? (Select four.)

A. create

B. open

C. archive

D. move

E. rename

F. run

**Answer:** ACDF

6. Upon which convention are custom Symantec Endpoint Protection Intrusion Prevention signatures

based?

A. Generic Exploit Blocking

B. Cisco IDS

C. SNORT

D. Tripwire

**Answer:** C

7. Symantec released a new version of Symantec Endpoint Protection client software. An administrator

needs to find out what versions of Symantec Endpoint Protection are currently in the network.

Which report provides this information?

A. Application and Device Control Report

B. System Report

C. Compliance Report

D. Computer Status Report

**Answer:** D

8. Where can you determine what content updates are available on the Symantec Endpoint Protection

Manager?

A. Home page

B. Monitors page

C. Clients page

D. Admin page

**Answer:** D

9. How does Symantec Endpoint Protection use Unmanaged Detector to find unmanaged devices on the network?

A. It compares MAC addresses to a list of known hosts.

B. It receives logon failures notifications from an LDAP server.

C. It pings clients on port 80 to trigger a response from managed clients.

D. It attempts to make http connections with clients in an address range.

**Answer:** A

10. What are three features of Symantec Endpoint Protection 11.0? (Select three.)

A. Application Performance Management

B. Client Firewall

C. Application and Device Control

D. Endpoint Change Control

E. Intrusion Prevention

**Answer:** BCE

11. How many client installation packages are required to install Symantec Endpoint Protection 11.0 with all available components?

A. one

B. two

C. three

D. four

**Answer:** A

12. What is a benefit of Symantec Endpoint Protection 11.0?

A. A single client provides all functions, which reduces the resource usage footprint.

B. Solaris is a supported platform for the client.

C. The number of required management consoles is reduced from five to three, which simplifies

administration compared to previous versions.

D. Proactive Threat Protection runs in real-time.

**Answer:** A


13. Which two roles can Symantec Endpoint Protection Manager assign to managed clients? (Select two.)

A. LAN Enforcer

B. Group Update Provider

C. Unmanaged Detector

D. Database Replicator

**Answer:** BC


14. Which two statements describe the interactions between Symantec Endpoint Protection 11.0 and

Quarantine Server? (Select two.)

A. Clients upload log data and quarantined files to Symantec Endpoint Protection Manager, which

forwards the files to the Quarantine Server.

B. Clients upload log data to Symantec Endpoint Protection Manager and upload quarantined files to

Quarantine Server.

C. Clients upload log data and quarantined files to the Quarantine Server, which forwards the log data to

the Symantec Endpoint Protection Manager.

D. Symantec Endpoint Protection Manager sends quarantine policies, which define the location of the

Quarantine Server, to managed clients.

E. The Quarantine Server sends its location and quarantine policies and rules to all clients.

**Answer:** BD


15. Which parameter is unique to each Symantec Endpoint Protection client?

A. CUID

B. GUID

C. SUID

D. RUID

**Answer:** B

16. Which two are characteristics of Proactive Threat Protection? (Select two.)

A. detects unknown threats

B. inspects encrypted network traffic

C. evaluates process behavior

D. blocks attacker's IP address

**Answer:** AC

17. Which two high-level components make up the Symantec Endpoint Protection solution? (Select two.)

A. Symantec Endpoint Protection

B. Symantec Critical System Protection

C. Symantec Security Information Manager

D. Symantec Network Access Control

**Answer:** AD

18. Which two do you need in order to add a Replication Partner? (Select two.)

A. local domain user and password

B. administrator name and password

C. local domain administrator name and password

D. replication server name and port

**Answer:** BD

19. Which failover option is available in Symantec Endpoint Protection?

A. One manager can fail over between two databases in a single site.

B. One client can fail over between two managers in a single site.

C. One manager can fail over to another Group Update Provider.

D. One client can fail over between two databases in separate sites.

**Answer:** B

20. What is the relationship of Symantec Network Access Control to Symantec Endpoint Protection 11.0?

A. Symantec Network Access Control is completely integrated with Symantec Endpoint Protection 11.0 and cannot be installed alone.

B. Symantec Network Access Control is a part of Symantec Endpoint Protection 11.0, but is not enabled unless a separate license is purchased.

C. Symantec Network Access Control is not part of Symantec Endpoint Protection 11.0, but does not interfere with Symantec Endpoint Protection 11.0 components.

D. Symantec Network Access Control works with Symantec Endpoint Protection 11.0, but uses a different management console and installation process.

**Answer:** B


21. How do requirements for installing Symantec Network Access Control relate to installing various components of Symantec Endpoint Protection 11.0?

A. It does NOT install on any host that is used as either the Symantec Endpoint Protection Manager or a Group Update Provider.

B. It installs in the same client package as all of the Symantec Endpoint Protection 11.0 components.

C. It does NOT install on any client unless Symantec Endpoint Protection 11.0 is installed.

D. It installs and is automatically enabled when the Network Threat Protection component of Symantec Endpoint Protection 11.0 is installed on any client.

**Answer:** B


22. Which two statements are true about Symantec Network Access Control? (Select two.)

A. It is integrated into Symantec Endpoint Protection 11.0, with a shared management console and a single shared client.

B. It is partially integrated into Symantec Endpoint Protection 11.0, with a shared management console and compatible clients.

C. It is integrated into and included with Symantec Endpoint Protection 11.0, but requires an additional license to enable the network access control features.

D. It is on the roadmap to be integrated with Symantec Endpoint Protection 11.0 in a future maintenance

pack release.

E. It is not integrated with Symantec Endpoint Protection 11.0, although both clients may be installed on any supported host without any operational issues.

**Answer:** AC

23. Which statement is true about Symantec Network Access Control 11.0 client administration?

A. The administration console for Symantec Network Access Control 11.0 has been updated to resemble the Symantec Endpoint Protection Manager console.

B. Symantec Network Access Control 11.0 centralized administration is now provided exclusively through the Symantec Endpoint Protection Manager console.

C. The administration console for Symantec Network Access Control 11.0 now includes fields and options that require that Network Threat protection is enabled.

D. Symantec Network Access Control 11.0 can now be administered through either its own console or the Symantec Endpoint Protection Manager console.

**Answer:** B

24. A company is interested in making sure that their remote VPN users have compliant systems before joining the corporate network.

Which two Symantec Network Access Control methods are recommended? (Select two.)

A. LAN Enforcer

B. Gateway Enforcer

C. Self Enforcement

D. DHCP Enforcer

**Answer:** BC

25. Which Symantec Network Access Control Enforcer can be deployed as either a software plug-in or as an appliance?

A. LAN Enforcer

B. Gateway Enforcer

C. Self Enforcement

D. DHCP Enforcer

**Answer:** D

26. On which two operating systems can you install Symantec Endpoint Protection Manager? (Select two.)

A. Microsoft Windows Vista Ultimate

B. Microsoft Windows NT Server

C. Microsoft Windows XP Professional

D. Microsoft Windows Server 2003

**Answer:** CD

27. What is the maximum number of clients that a single Symantec Endpoint Protection Manager can support?

A. 25,000

B. 50,000

C. 75,000

D. 100,000

**Answer:** B

28. Which component must be installed prior to installing Symantec Endpoint Protection Manager?

A. Apache Tomcat Server

B. Microsoft Internet Authentication Server (IAS)

C. Microsoft Internet Information Server (IIS)

D. Sun Java Runtime Environment (JRE)

**Answer:** C

29. What is the maximum number of clients that the embedded database can support?

A. 1,000

B. 2,000

C. 3,000

D. 5,000

**Answer:** A


30. Which two external databases does Symantec Endpoint Protection Manager support? (Select two.)

A. Microsoft SQL Server 2000

B. MySQL Server 2005

C. Microsoft SQL Server 2005

D. Oracle Database 11g

**Answer:** AC