



ST0-135

Symantec Network Access Control 12.1 Technical Assesment

Total Questions:

Document version: 8.04.11

Important Note About ST0-135 PDF

techeXams' **ST0-135 PDF** is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this exam questions. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. It's our guarantee.

Copyright

techeXams holds the copyright of this material. techeXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Question: 1.

What happens when the Symantec Endpoint Protection Manager is upgraded to include Symantec Network Access Control functionality?

- A. Network Access Control has to be enabled manually in the Manager.
- B. A Symantec Network Access Control Client is deployed to all clients.
- C. Clients without Host Integrity policies get dropped into Quarantine.
- D. The Host Integrity policy is enabled in the Policy Library.

Answer: D

Question: 2.

What are two primary purposes of Symantec Network Access Control? (Select two.)

- A. install new operating systems to client workstations
- B. update policies on the Symantec Endpoint Protection Manager
- C. prevent out-of-compliance systems from impacting production resources
- D. check endpoint computers' Host Integrity compliance periodically
- E. place a non-compliant endpoint into a captive portal

Answer: CD

Question: 3.

Which two enforcement modes can be configured on the Symantec 6100 appliance? (Select two.)

- A. LAN Enforcer
- B. DHCP Enforcer
- C. Integrated DHCP Enforcer
- D. Gateway Enforcer
- E. Self Enforcement

Answer: AD

Question: 4.

Which enforcement technology has the ability to deploy the On-Demand client?

- A. Integrated Enforcer for Microsoft Network Access Protection
- B. LAN Enforcer
- C. Integrated Enforcer for Microsoft DHCP Server
- D. Gateway Enforcer

Answer: D

Question: 5.

Which two databases are supported when Symantec Endpoint Protection Manager is being configured? (Select two.)

- A. Oracle Database 11g
- B. Microsoft SQL Server 2005, SP2
- C. Microsoft SQL Express, SP1
- D. Microsoft SQL Server 2008
- E. MySQL Database 5.5

Answer: BD

Question: 6.

A guest is unable to download the On-Demand client. The guest is running Windows 7 64-bit and connecting with the Mozilla Firefox browser. The computer has 512 MB RAM and 50 MB free disk space. What is the likely cause of the problem?

- A. The guest's system has insufficient disk space.
- B. The guest's browser is unsupported.
- C. The guest's operating system is unsupported.
- D. The guest's system has insufficient RAM.

Answer: A

Question: 7.

What is a characteristic of the Symantec Network Access Control Integrated Enforcer for Integrated Enforcers?

- A. It provides 802.1x enforcement.
- B. It is only available as a plug-in.
- C. It is installed as an appliance.
- D. It requires a DHCP Proxy.

Answer: B

Question: 8.

Which statement is true about Symantec Network Access Control compliance?

- A. It ensures that endpoints, such as clients and servers, meet specific administrator-defined requirements.
- B. It ensures the management of a secure client endpoint through the creation and implementation of group policies.
- C. It provides services needed by a client to bring itself up to spec in order to gain access to network resources.
- D. It provides clients with the ability to configure and deliver content and product updates to other clients in the same topological location.

Answer: B

Question: 9.

Which two components run Host Integrity checking? (Select two.)

- A. Symantec Endpoint Protection client
- B. Symantec Network Access Control LAN Enforcer
- C. Symantec Network Access Control On-Demand client
- D. Symantec Network Access Control Gateway Enforcer
- E. Symantec Critical System Protection client

Answer: AC

Question: 10.

Which enforcement method requires the least amount of effort to implement, can restrict network traffic if desired, and has the least impact on the customer network?

- A. Integrated Microsoft DHCP Enforcement
- B. Self Enforcement
- C. Gateway Enforcement
- D. LAN Enforcement

Answer: B

Question: 11.

How does the Gateway Enforcer function on the network?

- A. Layer 2 routing operation from external interface to internal interface
- B. Layer 2 bridging operation from external interface to internal interface
- C. Layer 3 bridging operation from external interface to internal interface
- D. Layer 3 bridging operation from internal to external interface

Answer: B

Question: 12.

Besides a LAN Enforcer, which two components are required for transparent mode? (Select two.)

- A. Symantec Endpoint Protection Manager
- B. VPN remote access device
- C. RADIUS server upstream of LAN Enforcer
- D. 802.1x capable switch
- E. ACLs and a firewall enabled in the Enforcer

Answer: AD

Question: 13.

When using Symantec Network Access Control Integrated Enforcer, which two additional components are required for guest access with Host Integrity checking? (Select two.)

- A. LAN Enforcer
- B. Gateway Enforcer
- C. Symantec Endpoint Protection Manager
- D. Microsoft IAS Server
- E. Microsoft Active Directory Domain Controller

Answer: BC

Question: 14.

Which two functions can Symantec Network Access Control Host Integrity check for and automate to reduce Help Desk calls for IT support? (Select two.)

- A. detect and prevent keystroke loggers from running
- B. ensure required software applications such as Altiris are running
- C. encrypt wireless communications for local administrative users
- D. start services that have been stopped by users
- E. query Insight reputation for a new file download

Answer: BD

Question: 15.

Which Symantec Network Access Control technology can prevent a device from connecting to the network and receiving an IP address?

- A. LAN Enforcer
- B. DHCP Enforcer
- C. Integrated Enforcer
- D. Self Enforcement

Answer: A

Question: 16.

Which components do Symantec Network Access Control and Symantec Endpoint Protection share?

- A. identical user interfaces and the same installer package
- B. the same location awareness policy
- C. the same Host Integrity policy and Replication policy
- D. the same manager, database schema, and infrastructure mechanics

Answer: B

Question: 17.

When using a non-Symantec (third party) anti-virus solution, which two types of Symantec clients can be used? (Select two.)

- A. Symantec On-Demand client
- B. Symantec Compliance Center client
- C. Symantec Network Access Control client
- D. Symantec Dissolvable client for Linux
- E. Symantec Critical System Protection client

Answer: AC

Question: 18.

A guest with a Macintosh laptop without Symantec Endpoint Protection installed connects to an organization's wireless access point to browse a website. The organization uses Symantec Network Access Control with the On-Demand agent feature turned on. Which behavior will the guest's laptop experience?

- A. It will be permanently denied all access to the network.
- B. It will be moved to quarantine VLAN.
- C. It will be redirected to an HTTP download page.

D. It will be given a quarantine IP address.

Answer: C

Question: 19.

What are two capabilities of the Symantec Network Access Control client? (Select two.)

- A. provide SONAR protection
- B. check for third party security software
- C. scan for viruses
- D. execute custom scripts
- E. provide Network Threat Protection

Answer: BD

Question: 20.

An employee has an employer-issued laptop with Symantec Endpoint Protection client installed. Symantec Network Access Control is enabled on the laptop. Employees are permitted to connect from a remote network to a corporate network via a VPN connection. The clients connect through a Gateway Enforcer to access the corporate network. What happens first when the employee connects to the corporate network from home through the VPN tunnel?

- A. An On-Demand client is downloaded.
- B. A LiveUpdate occurs to update Host Integrity templates.
- C. The client computer provides compliance information to the Gateway Enforcer.
- D. The client computer provides compliance information directly to the Symantec Endpoint Protection Manager.

Answer: C

Question: 21.

Which policy type does Symantec Network Access Control client use?

- A. Virus and Spyware

- B. Host Integrity
- C. Intrusion Prevention
- D. Application Control

Answer: B

Question: 22.

An organization that is deploying Symantec products needs to use network access control, antivirus and spyware, proactive threat protection, and network threat protection software. Which Symantec client(s) should be installed on the organization's workstations?

- A. Symantec Network Access Control client
- B. Symantec Network Access Control and Symantec Endpoint Protection clients
- C. Symantec Endpoint Protection client
- D. Symantec Endpoint Protection and the Symantec On-Demand clients

Answer: C

Question: 23.

An administrator has upgraded a Symantec Endpoint Protection Manager to include Symantec Network Access Control. How should the administrator deploy compliance checking to existing Symantec Endpoint Protection clients?

- A. Edit the client feature set to include compliance checking.
- B. Create compliance checking and add to the 'Location Specific Setting'.
- C. Create compliance checking policies on a per location basis.
- D. Edit the 'Client Install Setting' to include compliance checking.

Answer: C

Question: 24.

Symantec Network Access Control can be implemented standalone or as an integrated module of Symantec Endpoint Protection. What is the only policy that exists in both standalone and integrated implementations

- A. Host Integrity
- B. LiveUpdate
- C. Centralized Exceptions
- D. Firewall

Answer: B

Question: 25.

How many additional client packages become available when a Symantec Endpoint Protection Manager has been upgraded with Symantec Network Access Control?

- A. 0
- B. 1
- C. 2
- D. 3

Answer: C

Question: 26.

Where are Symantec Network Access Control client packages found on the Symantec Endpoint Protection Manager?

- A. Client > Policies
- B. Admin > Install Packages
- C. Policies > Policy Components
- D. Clients > Install Packages

Answer: B

Question: 27.

Which technology is contained in the Symantec Network Access Control agent?

- A. Firewall
- B. Intrusion Prevention

- C. Host Compliance
- D. Antivirus

Answer: C

Question: 28.

Which Symantec product can have Symantec Network Access Control functionality enabled?

- A. Symantec AntiVirus 10.2
- B. Symantec Client Security 3.0
- C. Symantec Critical System Protection 5.2
- D. Symantec Endpoint Protection 12.1

Answer: D

Question: 29.

When installing the Symantec Network Access Control with an external database, what needs to be installed on the Symantec Endpoint Protection Manager prior to installing the manager software?

- A. Microsoft IIS
- B. Apache Tomcat
- C. Microsoft SQL client tools
- D. Apache web server

Answer: C

Question: 30.

On which product can Symantec Network Access Control functionality be enabled?

- A. Symantec AntiVirus 10.2
- B. Symantec Client Security 3.1
- C. Symantec Critical System Protection 5.2

D. Symantec Endpoint Protection 12.1

Answer: B

Question: 31.

Which method can be used to upgrade a Symantec Endpoint Protection Manager to include Symantec Network Access Control functionality?

- A. Use add/remove programs.
- B. Perform a MSI push.
- C. Run the SNAC.exe.
- D. Run the Upgrade wizard.

Answer: D

Question: 32.

Which two components are included in the disaster recovery file? (Select two.)

- A. symlink.xml
- B. config.properties
- C. encryption password
- D. certificate files
- E. database

Answer: CD

Question: 33.

What is the Symantec recommended first step in upgrading the Symantec Endpoint Protection Manager to the next release?

- A. Turn off replication.
- B. Enable Local Authentication.
- C. Backup the database.
- D. Stop the Symantec Endpoint Protection Manager service.

Answer: C

Question: 34.

In a multi-site environment, which critical step must be manually taken prior to upgrading the Symantec Endpoint Protection Manager to the next major release?

- A. Stop the Symantec Endpoint Protection Manager service.
- B. Upgrade the Symantec Endpoint Protection client software.
- C. Turn off replication.
- D. Enable Local Authentication.

Answer: C

Get Full Version of Exam ST0-135 PDF Q&A

techeXams presents authentic, genuine and valid study material, which promise 100% success in very first attempt. To take optimal results for ST0-135 exam, you need to buy full version of ST0-135 question and answer. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. So come join us and quench your thirst for knowledge.

Get complete ST0-135 exam questions and answers by visiting URL

["http://www.techexams.ws/exams/ST0-135.do"](http://www.techexams.ws/exams/ST0-135.do)