250-315 Q&As

Administration of Symantec Endpoint Protection 12.1

Pass Symantec 250-315 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/250-315.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which Symantec Endpoint Protection defense mechanism provides protection against threats that propagate from system to system through the use of autorun.inf files?

A. Application and Device Control

B. SONAR

C. TruScan

D. Host Integrity

Correct Answer: A

QUESTION 2

An administrator uses ClientSideClonePrepTool to clone systems and virtual machine deployment.

What will the tool do when it is run on each system?

A. Run Microsoft SysPrep and removes all AntiVirus/AntiSpyware definitions

B. Disable Tamper Protect and deploys a Sylink.xml

C. Add a new Extended File Attribute value to all existing files

D. Remove unique Hardware IDs and GUIDs from the system

Correct Answer: D

QUESTION 3

An administrator needs to configure Secure Socket Layer (SSL) communication for clients. In the httpd.conf file, located on the Symantec Endpoint Protection Manager (SEPM), the administrator removes the hashmark (#) from the text string displayed below.

#Include conf/ssl/sslForcClients.conf

Which two tasks must the administrator perform to complete the SSL configuration? (Select two.)

A. edit site.properties and change the port to 443

B. restart the Symantec Endpoint Protection Manager Webserver service

C. change the default certificates on the SEPM and reboot

D. change the Management Server List and enable HTTPs

E. change the port in Clients > Group > Policies > Settings > Communication Settings and force the clients to reconnect

Correct Answer: BD

QUESTION 4

A company has an application that requires network traffic in both directions to multiple systems at a specific external domain. A firewall rule was created to allow traffic to and from the external domain, but the rule is blocking incoming traffic.

What should an administrator enable in the firewall policy to allow this traffic?

A. TCP resequencing

B. Smart DHCP

C. Reverse DNS Lookup

D. Smart WINS

Correct Answer: C

QUESTION 5

A company has a small number of systems in their Symantec Endpoint Protection Manager (SEPM) group with federal mandates that AntiVirus definitions undergo a two week testing period. After being loaded on the client, the tested virus definitions must remain unchanged on the client systems until the next set of virus definitions have completed testing. All other clients must remain operational on the most recent definition sets. An internal LiveUpdate Server has been considered as too expensive to be a solution for this company.

What should be modified on the SEPM to meet this mandate?

A. The LiveUpdate Settings policy for this group should be modified to use an Explicit Group Update Provider.

B. The LiveUpdate Content policy for this group should be modified to use a specific definition revision.

C. The SEPM site LiveUpdate settings should be modified so the Number of content revisions to keep is set to 1.

D. The SEPM site LiveUpdate settings should be modified so the Number of content revisions to keep is set to 14.

Correct Answer: B

QUESTION 6

An administrator is re-adding an existing Replication Partner to the local Symantec Endpoint Protection Manager site.

Which two parameters are required to re-establish this replication partnership? (Select two.)

A. remote server IP Address and port

B. remote site Encryption Password

C. remote site Domain ID

D. remote server Administrator credentials

E. remote SQL database account credentials

Correct Answer: AD

QUESTION 7

Administrators at a company share a single terminal for configuring Symantec Endpoint Protection. The administrators want to ensure that each administrator using the console is forced to authenticate using their individual credentials. They are concerned that administrators may forget to log off the terminal, which would easily allow others to gain access to the Symantec Endpoint Protection Manager (SEPM) console.

Which setting should the administrator disable to minimize the risk of non-authorized users logging into the SEPM console?

A. allow users to save credentials when logging on

B. delete clients that have not connected for specified time

C. lock account after the specified number of unsuccessful logon attempts

D. allow administrators to reset the passwords

Correct Answer: A

QUESTION 8

Refer to the exhibit.

An administrator uses the search criteria displayed in the exhibit. Which results are returned from the query?

A. all Windows 2012 Servers in the Default Group

B. only VMware Servers in the Default Group

C. all Windows 2012 Servers and all Virtualized Servers in the Default Group

D. only Windows 2012 Servers that are Virtualized in the Default Group

Correct Answer: D

QUESTION 9

An administrator is troubleshooting a Symantec Endpoint Protection (SEP) replication.

Which component log should the administrator check to determine whether the communication between the two sites is working correctly?

A. Apache Web Server

B. Tomcat

C. SQL Server

D. Group Update Provider (GUP)

Correct Answer: B

QUESTION 10

Which tool should the administrator run before starting the Symantec Endpoint Protection Manager upgrade as a Symantec Best Practice?

A. collectLog.cmd

B. DBValidator.bat

C. LogExport.cmd

D. Upgrade.exe

Correct Answer: B

QUESTION 11

In the virus and Spyware Protection policy, an administrator sets the First action to Clean risk and sets If first action fails to Delete risk.

Which two factors should the administrator consider? (Select two.)

A. The deleted file may still be in the Recycle Bin.

B. IT Analytics may keep a copy of the file for investigation.

C. False positives may delete legitimate files.

D. Insight may back up the file before sending it to Symantec.

E. A copy of the threat may still be in the quarantine.

Correct Answer: CE

QUESTION 12

A financial company enforces a security policy that prevents banking system workstations from connecting to the Internet.

Which Symantec Endpoint Protection technology is ineffective on this company\\'s workstations?

A. Insight

B. Intrusion Prevention

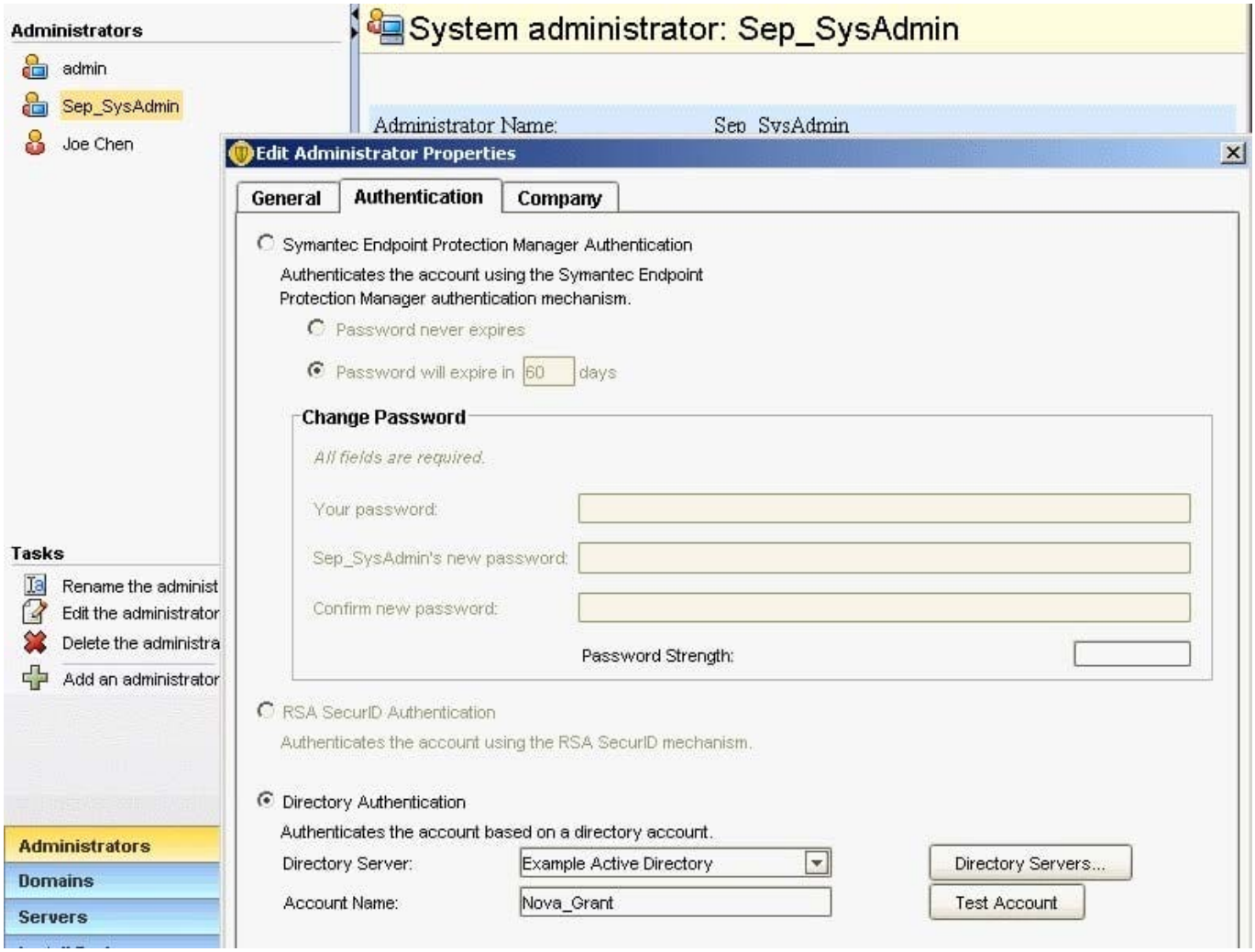
C. Network Threat Protection

D. Browser Intrusion Prevention

Correct Answer: A

QUESTION 13

Refer to the exhibit.



An administrator has configured the Symantec Endpoint Protection Manager (SEPM) to use Active Directory authentication. The administrator defines a new Symantec Endpoint Protection administrator named Sep_SysAdmin, configured to use Directory Authentication.

Which password needs to be entered when the administrator logs in to the SEPM console as Sep_SysAdmin?

A. The password for the Active Directory account Nova_Grant

B. The password for the SEPM account Nova_Grant

C. The password for the Active Directory account Sep_SysAdmin

D. The password for the SEPM account Sep_SysAdmin

Correct Answer: A

QUESTION 14

A company deploys Symantec Endpoint Protection client to its sales staff who travel across the country. Which deployment method should the company use to notify its sales staff to install the client?

A. Push mode

B. Client Deployment Wizard

C. Pull mode

D. Unmanaged Detector

Correct Answer: B

QUESTION 15

An administrator receives a browser certificate warning when accessing the Symantec Endpoint Protection Manager (SEPM) Web console.

Where can the administrator obtain the certificate?

A. SEPM console Licenses section

B. Admin > Servers > Configure SecureID Authentication

C. SEPM console Admin Tasks

D. SEPM Web Access

Correct Answer: D