IBM 000-533

IBM Security SiteProtector V2.0 SP8.1 System

Version: 5.0

QUESTION NO: 1

Which option addresses a customer environment receiving more than 5,000,000 events and 300,000 heartbeats per day for IBM Security SiteProtector Systems V2.0 SP8.1 (SiteProtector)?

A. plan for an additional site and divide the load
B. add 100 GB of available disk space to the database
C. plan for an addition Event Collector / Agent Manager pair
D. upgrade the CPU on the SiteProtector Application Server

Answer: A
Explanation:

QUESTION NO: 2

In what format does the Event Archiver store events?

A. as flat files in the file system
B. as records in a local SQL database
C. as records in a remote SQL database
D. in memory queue for the Event Collector

Answer: A
Explanation:

QUESTION NO: 3

How many computer(s) does the Recommended option install on in the Deployment Manager?

A. 1
B. 2
C. 3
D. 4

Answer: B
Explanation:

QUESTION NO: 4

Which two items are important considerations for performance? (Choose two.)

A. agent events per day
B. agent purges per day
C. agent updates per day

D. agent heartbeats per day
E. agent installations per day

Answer: A,D
Explanation:

QUESTION NO: 5

According to the IBM Security SiteProtector Systems V2.0 SP8.1 scalability guidelines, what is the maximum event rate and maximum heartbeat rate per day for a small deployment?

A. 25,000 events / 500 heartbeats
B. 50,000 events / 1,000 heartbeats
C. 100,000 events / 5,000 heartbeats
D. 125,000 events / 7,000 heartbeats

Answer: B
Explanation:

QUESTION NO: 6

What is a primary function of the IBM Security SiteProtector Systems V2.0 SP8.1 Core?

A. event data storage
B. command and control
C. correlate attack information
D. receive and process agent heartbeats

Answer: B
Explanation:

QUESTION NO: 7

Which three operating systems meet the requirements for installing the IBM Security SiteProtector Systems V2.0 SP8.1 Database in the Recommended option? (Choose three.)

A. Windows XP Professional SP2
B. Windows Server 2008 Standard
C. Windows 2000 Advanced Server
D. Windows Server 2008 Enterprise
E. Windows Server 2003 Enterprise Edition
F. Windows Server 2003 SP2 Standard Edition

Answer: B,D,F

Explanation:

QUESTION NO: 8

Which three versions of Microsoft SQL Server meet the requirements for installing the IBM Security SiteProtector Systems V2.0 SP8.1 Database in the Recommended option? (Choose three.)

A. SQL Server 2000 64-bit Edition
B. SQL Server 2005 Standard Edition
C. SQL Server 2000 Standard Edition
D. SQL Server 2008 Standard Edition
E. SQL Server 2003 Enterprise Edition
F. SQL Server 2008 Enterprise Edition

Answer: B,D,F
Explanation:

QUESTION NO: 9

How much system hard drive space is required for the IBM Security SiteProtector Systems V2.0 SP8.1 Database in the Recommended option?

A. 9 GB
B. 18 GB
C. 27 GB
D. 36 GB

Answer: B
Explanation:

QUESTION NO: 10

Which default network port must be open from the Agent Manager to the Application Server?

A. 901
B. 902
C. 8443
D. 3995

Answer: D
Explanation:

QUESTION NO: 11

Which two required network ports must be open for successful communication between the IBM Security SiteProtector Systems V2.0 SP8.1 Application Server and the Event Collector? (Choose two.)

A. 902
B. 914
C. 3995
D. 8996
E. 2998

Answer: D,E

Explanation:

QUESTION NO: 12

Which two virtual platforms are supported for running IBM Security SiteProtector Systems V2.0 SP8.1? (Choose two.)

A. Windows Virtual PC
B. VMware ESX Server V4.x
C. VMware ESX Server V3.x
D. VMware Workstation V7.1
E. Microsoft Virtual Server 2003

Answer: B,C

Explanation:

QUESTION NO: 13

According to the scalability guidelines for a large site, a customer should have at least what speed hard disks available to the database server?

A. 5400 RPM
B. 7200 RPM
C. 10000 RPM
D. 15000 RPM

Answer: D

Explanation:

QUESTION NO: 14

The customer is performing a large installation. What is the disk size for the database server

according to the scalability guidelines?

A. 50 GB - 73 GB
B. 74 GB - 142 GB
C. 143 GB - 730 GB
D. 731 GB - 999 GB

Answer: C
Explanation:

QUESTION NO: 15

What are the default emergency purge settings for IBM Security SiteProtector Systems V2.0 SP8.1 in an Express installation?

A. 85% Threshold / 5% Purge Margin
B. 55% Threshold / 20% Purge Margin
C. 65% Threshold / 15% Purge Margin
D. 75% Threshold / 10% Purge Margin

Answer: A
Explanation:

QUESTION NO: 16

The customer is planning to deploy 50,000 desktops. At a minimum, how many standalone Event Collector / Agent Manager pairs should be configured to communicate with the database?

A. 1
B. 2
C. 3
D. 4

Answer: C
Explanation:

QUESTION NO: 17

A customer has deployed an Express installation. What is the default action when the database reaches 85% of capacity?

A. The database will continue processing normally without purging.
B. The database will begin purging up to 5% of the oldest data from the database.
C. The database will begin purging up to 10% of the oldest data from the database.

D. The database will begin purging up to 15% of the oldest data from the database.

Answer: B
Explanation:

QUESTION NO: 18

A customer wants to create daily backups but does not have a large amount of disk space available to maintain transaction logs. Which SQL recovery model should be configured?

A. Full
B. Simple
C. Closed
D. Complete

Answer: B
Explanation:

QUESTION NO: 19

A corporation is deploying IBM Security SiteProtector Systems V2.0 SP8.1 (SiteProtector) and plans to use Enterprise Scanner to scan their various offices across the world each with their own assessment policy. In addition, each country and region may have different requirements which will need to be assessed. Which top to bottom group structure hierarchy best satisfies their needs?

A. Country > Region > Office
B. Region > Office > Country
C. Office > Country > Region
D. Office > Region > Country

Answer: A
Explanation:

QUESTION NO: 20

A corporation is deploying IBM Security SiteProtector Systems V2.0 SP8.1 and plans to use Enterprise Scanner to scan their various business departments each with their own assessment policy. Additionally, network subnets may require a different policy within each department. Which top to bottom group structure hierarchy best satisfies their needs?

A. ACME > Department > Subnet
B. Subnet > Department > ACME
C. Subnet > ACME > Department