HP HP0-M55

ArcSight ESM Administrator

Version: 4.0

QUESTION NO: 1

What must be done first to restore the database from an online backup?

A. run the Oracle restore wizard
B. ensure that the archived redo logs are located in the archive log destination
C. bring the affected tablespaces online
D. reinstall the Oracle installation

Answer: B
Explanation:

QUESTION NO: 2

What happens when a Connector upgrade that was initiated from within the ArcSight Console fails?

A. The Connector automatically rolls back to the previously working version.
B. The Connector does not respond to the failed upgrade.
C. The Connector reports to the Manager that the upgrade failed and then died.
D. The Connector automatically attempts the upgrade again.

Answer: A
Explanation:

QUESTION NO: 3

With regard to SmartConnectors, what is roll back?

A. collecting cached data after a communication failure
B. uninstallation of a package in the event of failure
C. a way to revert to the previous version of a Connector when a Connector upgrade fails
D. a way to gather data that has moved beyond the archive window

Answer: C
Explanation:

QUESTION NO: 4

Which statement is true about starting and stopping ArcSight SmartConnector services?

A. They are started and stopped independently of the other ArcSight component services.
B. The order in which they are started and stopped is based on event flow.
C. How they are started and stopped depends on whether or not the ArcSight Manager is running.
D. They are started and stopped in conjunction with the Oracle database services.

Answer: A
Explanation:

QUESTION NO: 5

What is a trust store (sometimes called a key store)?

A. the preferred source for obtaining signed certificates
B. a list of trusted Certificate Authorities
C. the location of a system's private keys
D. the set of backup files containing SSL information

Answer: B
Explanation:

QUESTION NO: 6

Which key pair types are valid selections when using the Manager Setup Wizard to create an SSL key pair? (Select two.)

A. non-expiring SSL key pair
B. self-signed key pair
C. demo key pair
D. random generator key pair

Answer: B,C
Explanation:

QUESTION NO: 7

During Connector install, which statement is true about the ArcSight Manager's host name or IP

address?

A. It must match the host name or IP address in the ArcSight Manager's SSL certificate.
B. The host name or IP address is used as an encryption key.
C. It can be any legitimate host name or IP address.
D. It must contain a combination of alpha-numeric characters.

Answer: A
Explanation:

QUESTION NO: 8

What are ArcSight Foundations?

A. user groups organized to explore and share ideas for extending ArcSight ESM capabilities
B. coordinated resources that provide monitoring, analysis, and reporting capabilities
C. categories of resources used for monitoring ArcSight system health and status
D. packages that are installed but cannot be modified

Answer: B
Explanation:

QUESTION NO: 9

Which ArcSight Foundation should you use to identify traffic and bandwidth usage?

A. Configuration Monitoring
B. Intrusion Monitoring
C. ArcSight Administration
D. Network Monitoring

Answer: D
Explanation:

QUESTION NO: 10

Which ArcSight Foundation should you use to identify and analyze unexpected modifications to systems, devices, or applications?

A. Configuration Monitoring
B. Intrusion Monitoring
C. ArcSight Administration
D. Network Monitoring

Answer: A
Explanation:

QUESTION NO: 11

There are three types of ArcSight SmartConnectors. Which type is used primarily to execute commands on a device to retrieve, modify, or analyze its configuration?

A. Event Connectors
B. Scanner Connectors
C. CounterACT Connectors
D. SNMP Connectors

Answer: C
Explanation:

QUESTION NO: 12

Which file types MUST be included in an Oracle backup? (Select two.)

A. table files
B. data files
C. program files
D. configuration files

Answer: B,D
Explanation:

QUESTION NO: 13

How can you restore a new ArcSight Web installation to a previous configuration?

A. copy the old ArcSight Web installation's config directory and cacerts file into the new installation

B. copy the ArcSight Manager's config directory into the new installation
C. manually reconfigure the new installation
D. connect to the Manager and download the saved configuration

Answer: A
Explanation:

QUESTION NO: 14

In Network Modeling, what is closest to being a subnet?

A. zone
B. network
C. Asset Range
D. Network Range

Answer: A
Explanation:

QUESTION NO: 15

Which components does a Network Model include? (Select two.)

A. assets
B. data monitors
C. dashboards
D. zones

Answer: A,D
Explanation:

QUESTION NO: 16

In Network Modeling, what are SmartConnectors bound to? (Select two.)

A. zones
B. networks
C. devices

D. customers

Answer: B,D

Explanation:

QUESTION NO: 17

What is a Network Model?

A. a representation of the nodes on a network and certain characteristics of the network itself
B. a preconfigured resource used to set up ArcSight zones and communication paths
C. a dashboard containing data monitors for network, zone, asset, and customer monitoring
D. a diagram of network interface points and vulnerabilities

Answer: A

Explanation:

QUESTION NO: 18

Package bundles are exported with which file extension?

A. .xml file
B. .exe file
C. .msc file
D. .arb file

Answer: D

Explanation:

QUESTION NO: 19

Which command is used to modify retention periods?

A. Arcsight archive install
B. Arcsight database create
C. Arcsight retention create
D. Arcsight database pc

Answer: D

Explanation:

QUESTION NO: 20

What is an offline partition?

A. a partition that resides within the database
B. a partition that exceeds the online retention threshold and is therefore archived
C. a partition reserved for a future date
D. data that is no longer needed by ESM

Answer: B

Explanation:

QUESTION NO: 21

Which statements are true about retention areas? (Select two.)

A. Retention policies cannot be changed once they are set.
B. Retention areas can be configured using the Partition Management Wizard.
C. If the size of a retention area is reduced, the data outside of the retention area is automatically backed up.
D. Archived partitions outside the offline archive period become invalid.

Answer: B,D

Explanation:

QUESTION NO: 22

When configuring the ArcSight Database, what is the result of setting the offline archive period (Days) to Zero?

A. Partition Archiving is enabled.
B. Partition Archiving is disabled.
C. Online retention is enabled.
D. Online reserved period is enabled.

Answer: B
Explanation:

QUESTION NO: 23

What does Partition Archiving allow you to specify?

A. the number of partitions to keep offline
B. the number of partitions that remain online
C. the compression ratio to be used in partitioning
D. the amount of data to store in a partition

Answer: A
Explanation:

QUESTION NO: 24

What is the Reserve Period?

A. the amount of time to allow before compressing event data for storage
B. the number of future partitions to be maintained
C. the amount of time to wait before determining that a device is not operating
D. the maximum length of time archived partitions will be stored

Answer: B
Explanation:

QUESTION NO: 25

What is stored in a database partition?

A. as much data as it can hold
B. a user-configurable number of events
C. events from a one week time period
D. events from a 24-hour time period

Answer: D
Explanation:

QUESTION NO: 26

When can the online partition compression task fail? (Select two.)

A. when the partition being compressed is too old
B. when events are inserted into the partition that is being compressed
C. when the compression task takes more than two hours to complete
D. when the partition compressor does not have the necessary file permissions

Answer: B,C
Explanation:

QUESTION NO: 27

You are unable to see events from a specific device in the Console. The Active Channel filters are not the cause. Which component should you examine next in order to troubleshoot this issue?

A. Database
B. SmartConnector
C. Console
D. Device

Answer: B
Explanation:

QUESTION NO: 28

Which statements are true about SmartConnectors and batching? (Select two.)

A. Batches can be sent when they reach a certain size.
B. Batches can be sent on command.
C. Batches can be sent in priority order by severity.
D. Batches can be sent by Connector type.

Answer: A,C
Explanation:

QUESTION NO: 29

Preserve Raw Events, Turbo Mode, and Limit Event Processing Rate are all examples of which type of Connector options?

A. Processing options
B. Aggregation options
C. Filter conditions
D. Preservation options

Answer: A
Explanation:

QUESTION NO: 30

Which document provides the most detailed instructions for applying an Oracle CPU?

A. Oracle CPU release notes
B. ArcSight ESM Administrator's Guide
C. Opatch Readme file
D. ArcSight ESM Installation Guide

Answer: A
Explanation:

QUESTION NO: 31

What is a bundle?

A. a set of resources that makes up a package
B. a data transmission containing SSL information
C. a set of raw log events before they are parsed
D. a container for one or more packages

Answer: D
Explanation:

QUESTION NO: 32

Which method is used to back up an Oracle database without shutting down the database?

A. sequential backup
B. standalone backup
C. online backup
D. offline backup

Answer: C
Explanation:

QUESTION NO: 33

Which command should you use to configure notification acknowledgements after the initial configuration of ArcSight ESM?

A. arcsight managersetup
B. arcsight notifysetup
C. arcsight notifyconfig
D. arcsight setupnotify

Answer: A
Explanation:

QUESTION NO: 34

What are capabilities of the ArcSight Manager? (Select two.)

A. receives event data from SmartConnectors
B. normalizes events from devices
C. performs advanced event correlation and analysis
D. allows users to perform security monitoring through a built-in web interface

Answer: A,C
Explanation:

QUESTION NO: 35

Which statement is true about the ArcSight Web Server?

A. It is not required.
B. It is required if users will be accessing ESM through a web browser.
C. It should always be installed on the same server as the ArcSight Manager.
D. It can be used to create rules and view reports.

Answer: B
Explanation:

QUESTION NO: 36

Which command is used to add a secondary destination to a Connector's configuration?

A. arcsight destinations -n
B. arcsight connectorsetup -w
C. arcsight connectionwizard
D. arcsight connector -d

Answer: B
Explanation:

QUESTION NO: 37

Using SSL technology, information can be communicated over an encrypted channel. What is SSL?

A. Secure Sockets Layer
B. Security Standards Layer
C. Smart Stealth Layer
D. Standard Security Layer

Answer: A
Explanation:

QUESTION NO: 38

Which are clients of the ArcSight Manager? (Select two.)

A. ArcSight Correlation Engine
B. ArcSight Web
C. ArcSight SmartConnectors
D. ArcSight Database

Answer: B,C
Explanation:

QUESTION NO: 39

One of the benefits of SSL technology is authentication. What does authentication do?

A. validates client logins using advanced identity detection technology
B. encrypts information sent between clients and servers
C. adds a hashing algorithm to prevent data modification between client and server
D. ensures that clients send information to the actual intended server, not a machine pretending to be that server

Answer: D
Explanation:

QUESTION NO: 40

What is the default port used when connecting to the ArcSight Web interface?

A. TCP 9443
B. UDP 9443
C. TCP 8443
D. UDP 8443

Answer: A
Explanation:

QUESTION NO: 41

What is the default port used by the ArcSight ESM Console to connect to the ArcSight Manager?

A. TCP 8443

B. UDP 8443
C. TCP 9443
D. UDP 9443

Answer: A
Explanation:

QUESTION NO: 42

What is the default port used to connect the ArcSight Manager to the ArcSight ESM Database (Oracle)?

A. 443
B. 1443
C. 1521
D. 8443

Answer: C
Explanation:

QUESTION NO: 43

The ArcSight Web release version must be the same version as what?

A. ArcSight Manager
B. ArcSight Database
C. ArcSight SmartConnectors
D. ArcSight Console

Answer: A
Explanation:

QUESTION NO: 44

What must you do prior to applying a patch to the ArcSight Manager?

A. stop the ArcSight Manager service
B. shut down all ArcSight SmartConnectors

C. delete all files in the tmp directory
D. disconnect the network cable

Answer: A
Explanation:

QUESTION NO: 45

What do the start and end times associated with a notification destination indicate?

A. the period of time the system will wait for a notification response
B. the period of time during which the destination is expected to respond
C. the period of time during which the notification can be sent
D. the period of time during which the notification can be received

Answer: C
Explanation:

QUESTION NO: 46

Which actions might the whine daemon initiate? (Select two.)

A. sending a message to the admin consoles
B. sending SNMP traps to a monitoring station
C. sending syslog messages to a syslog server
D. writing an event to the server.log file

Answer: A,D
Explanation:

QUESTION NO: 47

What are potential ways of acknowledging notifications? (Select two.)

A. by replying to notification email
B. by calling in to the notification response hotline
C. by sending email to SysAdmin
D. by using the Notifications Manager in the ArcSight Console

Answer: A,D
Explanation:

QUESTION NO: 48

Which statement is true about ArcSight SmartConnectors acting in "passive" mode?

A. They receive events forwarded from originating devices.
B. They pull events from originating devices.
C. They do not process events from devices.
D. They process events for performance testing but then discard them.

Answer: A
Explanation:

QUESTION NO: 49

Which statement is true about Connectors that are in a Paused state?

A. Paused Connectors are responding to the Manager but not sending or caching events.
B. Paused Connectors are responding to the Manager but events are being cached.
C. Paused Connectors are responding to the Manager and sending events.
D. Paused Connectors are not responding to the Manager.

Answer: B
Explanation:

QUESTION NO: 50

ArcSight SmartConnectors send event data directly to what?

A. ArcSight Manager
B. ArcSight Console
C. ArcSight Web Server
D. ArcSight Database

Answer: A
Explanation:

QUESTION NO: 51

Which command is used to check the status of the TNS Listener?

A. lsnrctl status
B. listener status
C. tnsstat
D. oralistener status

Answer: A
Explanation:

QUESTION NO: 52

Which ArcSight Manager directory should be backed up in order to preserve the server.properties file?

A. user directory
B. config directory
C. properties directory
D. jre directory

Answer: B
Explanation:

QUESTION NO: 53

What is the name of the resource you can use to override the default ArcSight mapping IP addresses to geographic regions?

A. zones
B. destinations
C. locations
D. categories

Answer: C
Explanation:

QUESTION NO: 54

What does the ArcSight Manager use to automatically establish identity, ownership, and criticality of the assets installed on a network?

A. Asset Types
B. Asset Groups
C. Asset Categories
D. Asset Ranges

Answer: C
Explanation:

QUESTION NO: 55

Which three attributes are used to describe an Asset Model?

A. vulnerabilities, locations, and asset categories
B. locations, asset categories, and threats
C. asset types, asset categories, and locations
D. vulnerabilities, addresses, and threats

Answer: A
Explanation:

QUESTION NO: 56

Which statements are true about user groups? (Select two.)

A. They can be based on departments, permission levels, or roles.
B. They control which users are allowed to log in to the Console.
C. They can be nested within other user groups.
D. They are enabled or disabled using Access Control Lists.

Answer: A,C
Explanation:

QUESTION NO: 57

Which statements are true about user groups and resources? (Select two.)

A. Resources are only visible to a user if the user's group has "Read" permissions for the resource.
B. A group with "inspect" permission enabled allows all users in that group to edit resources.
C. To change a user's permission to access a resource group, you either change the permissions of the user's group or put the user in a new group with different permissions.
D. A resource can only be accessed by a user if the user's group has "viewer" permissions for the resource.

Answer: A,C
Explanation:

QUESTION NO: 58

Which tablespace is used by ArcSight to store resources?

A. ARC_EVENT_DATA
B. ARC_SYSTEM_INDEX
C. ARC_SYSTEM_DATA
D. ARC_EVENT_INDEX

Answer: C
Explanation:

QUESTION NO: 59

Which statement is true about ArcSight Database structures?

A. Data tablespaces typically use more disk space than indices.
B. Indices typically use more disk space than data tablespaces.
C. There is no appreciable difference between index and data tablespaces.
D. The system data tablespace is always much larger than the event data tablespace.

Answer: B
Explanation:

QUESTION NO: 60

Which statement is true about SmartConnectors and FlexConnectors?

A. FlexConnectors allow creation of SmartConnectors that are tailored to individualized custom situations and specific security event data.
B. FlexConnectors are plug-and-play, self-programming SmartConnectors.
C. SmartConnectors do not include tools for customizing FlexConnectors.
D. SmartConnectors are vendor-specific and must be purchased through the individual device vendors.

Answer: A
Explanation: