PassQueen
a.k.a dumpsqueen.com

Administration of Symantec Client Management Suite 8.5

Symantec 250-447

Version Demo

Total Demo Questions: 16

Total Premium Questions: 169

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which two (2) critical pieces of information should an administrator consider when working with organizational views and organizational groups? (Select two.)

A. A resource can be contained by multiple organizational views

B. A resource can be assigned to multiple organizational groups within an organizational view

C. A resource can be contained by only one organizational view

D. A resource can be contained by only one organizational group within an organizational view

E. A resource can be assigned to only one organizational group within an organizational view

ANSWER: A

Explanation:

A resource can be contained by multiple organizational views. Organizational views in Symantec Client Management Suite provide alternative, business-oriented ways to arrange the same resource data, such as by department, location, cost center, or administrative responsibility. They do not create separate copies of the resource; instead, they provide separate organizational contexts in which that resource can be managed and reported on. This design lets an administrator place a computer, user, or other resource into each applicable view when the organization needs more than one way to represent its structure. For example, a device can be represented in a geographic view and also in a departmental view, allowing administrators to navigate and manage it through either business model. Understanding that views are not mutually exclusive is important when designing organizational structures and determining where administrators will locate resources. Symantec's Client Management Suite documentation describes organizational views as mechanisms for organizing resources according to an organization's needs and management structure. See the Client Management Suite 8.5 documentation and the Broadcom Knowledge Base for product documentation and organizational-management guidance.

QUESTION NO: 2

What task, if completed, will likely fix many of the performance related issues an administrator may experience in an IT Management Suite implementation, when solving a database performance related issues?

A. Implement a MS SQL Server Performance plan

B. Implement a MS SQL Server Defragmentation plan

C. Implement a MS SQL Server Optimization plan

D. Implement a MS SQL Server Maintenance plan

ANSWER: D

Explanation:

Implement a MS SQL Server Maintenance plan is correct because the Notification Server database is central to IT Management Suite operations, including collecting inventory and status data, processing reports, executing scheduled tasks, and serving console queries. As the database grows, index fragmentation and stale optimizer statistics can cause SQL Server to perform inefficient reads, choose poor query plans, and take longer to complete the data-processing work generated by managed endpoints.

A properly scheduled SQL Server maintenance plan provides a repeatable way to perform essential database upkeep. Depending on the environment and maintenance-window requirements, this commonly includes database-integrity checks, index reorganization or rebuilding, statistics updates, cleanup of historical backup files, and database backups. These activities improve the reliability of the database and help SQL Server access IT Management Suite data efficiently, which can resolve or substantially reduce many symptoms perceived as console, report, task-processing, or overall platform performance problems.

Maintenance must be scheduled appropriately for the database size and workload so that maintenance activity itself does not interfere with production processing. Microsoft documents the available maintenance-plan tasks at SQL Server Maintenance Plans; Broadcom's product documentation is available through the IT Management Suite documentation portal.

QUESTION NO: 3

An administrator must deploy software to a user´s computer to remedy a problem. The administrator is trying to determine whether to create a policy or a task to deploy the software to the user´s computers. In which two situations should the admin choose a policy instead of a task? (Select 2)

A. When actions are recurring

B. When actions are to be performed on a Schedule

C. When actions are to be performance on only a few resources

D. When actions are to be performed only once

E. When actions needs to be performed in near-real time

ANSWER: A B

Explanation:

Policies are the appropriate delivery mechanism when the desired action is recurring and when it must be performed on a schedule. In Symantec Client Management Suite, a policy represents an ongoing administrative intent: it remains assigned to its target and the Symantec Management Agent continues to evaluate the policy over time. This makes policies suitable for software deployment requirements that must be maintained or repeated rather than treated as a single, discrete operation.

For recurring actions, the policy model lets the administrator define the software-delivery configuration once and have managed computers continue to receive and evaluate it while they are members of the target. For scheduled actions, policy schedules provide predictable timing for policy evaluation and execution, helping administrators control when deployment activity occurs. This approach is particularly useful where a deployment must be consistently enforced across the applicable user-computer targets over an extended period.

Symantec's IT Management Suite documentation distinguishes policy-based, ongoing management from task-based execution and describes software-management deployment mechanisms and scheduling behavior. See the IT Management Suite 8.5 documentation and the Broadcom knowledge base for related product guidance.

QUESTION NO: 4

Which website should an administrator browse to when solving Task Service Installation issues to check that the task server is up and running?

A. https://SiteServer/Altiris/ClientTaskServer/

B. https://SiteServer/Symantec/TaskServer/

C. https://SiteServer/Altiris/TaskServer/

D. https://SiteServer/ClientTaskServer/

ANSWER: A

Explanation:

`https://SiteServer/Altiris/ClientTaskServer/` is the Task Server web endpoint used to confirm that the Task Server installation on a site server is available and responding. In Client Management Suite, Task Server is installed as a site-service component and provides the client-facing service used to receive and process task-related work. Browsing to this endpoint is therefore a direct, practical installation troubleshooting check: if the site server resolves, HTTPS is available,

and the ClientTaskServer application responds, the administrator has evidence that the Task Server web application is running under the Site Server's IIS configuration.

The `Altiris` virtual directory is significant because it is the standard web application path used by the Symantec Management Platform for site-server services. This check is particularly useful after installing, repairing, or upgrading Task Server, and when task execution appears not to reach managed computers. It complements checking the Task Server service status, IIS application pools, Site Server configuration, and relevant task-server logs. Broadcom's IT Management Suite documentation describes Task Server as the component that enables task execution on managed computers and documents the related site-server architecture and administration workflow. See the Broadcom IT Management Suite documentation and the Broadcom Knowledge Base for Task Server installation and troubleshooting guidance.

QUESTION NO: 5

An administrator is preparing to deploy Microsoft software updates by using Patch Management Solution.

Which two (2) actions are required to make imported Windows patch data available for deployment to managed computers? (Select two.)

A. Import Windows patch data

B. Create and enable a Software Update policy

C. Create a software catalog item

D. Run a hardware inventory policy

E. Create a Maintenance Window policy for the Notification Server

ANSWER: A B

Explanation:

The administrator must **import Windows patch data** and **create and enable a Software Update policy**. The patch-data import process downloads and imports the software bulletin and update metadata that Patch Management Solution uses to assess applicability and build software update policies.

After patch data is available, the administrator creates a Software Update policy, selects the required updates, targets the appropriate managed computers, and enables the policy. The Software Update Plug-in on managed computers then evaluates applicable updates and installs them according to the policy configuration. See the Broadcom Patch Management Solution documentation.

QUESTION NO: 6

In which two (2) locations should an administrator install the Symantec Installation Manager to facilitate the installation of IT Management Suite 8.5 on the target Notification Server? (Select two.)

A. On the server that is to be the Notification Server to create an offline installation if this Notification Server has no internet access

B. On another server to remotely install it on the target Notification Server

C. On the server that is to be the Notificat ion Server

D. It should be installed on a desktop class system to remotely install it on the target Notification Server

E. On another computer to create an offline installation package if the Notification Server has no internet access

ANSWER: C E

Explanation:

Symantec Installation Manager can be installed directly on the computer designated to become the Notification Server. This is the normal connected-installation approach: Installation Manager runs locally, obtains the required IT Management Suite installation resources, checks prerequisites, and installs the selected products and solutions on that server. Therefore, “On the server that is to be the Notificat ion Server” identifies a supported installation location.

For an isolated Notification Server without Internet access, Installation Manager can instead be installed on a separate computer that has Internet access. From that computer, the administrator creates an offline installation package containing the required product components and installation data, then makes that package available to the target Notification Server for installation. Thus, “On another computer to create an offline installation package if the Notification Server has no internet access” is also correct. These two locations support the respective connected and disconnected deployment workflows documented for IT Management Suite installation. See the IT Management Suite 8.5 documentation and the Broadcom Knowledge Base for Installation Manager and offline-installation guidance.

QUESTION NO: 7

A virtualized application on a client computer is corrupted. Which action can an administrator perform to fix the problem?

A. Deactivate and Reset

B. Deactivate and Reinstall

C. Delete and Reset

D. Reset and Reinstall

ANSWER: A

Explanation:

Deactivate and Reset is the appropriate corrective action for a corrupted virtualized application. Virtualized applications are delivered as managed software layers, which can be activated or deactivated independently of the base operating system. Deactivating the layer first removes the layer’s active virtualized view from the client, ensuring that files, registry entries, and application resources supplied through the layer are no longer in use. The reset action then restores the layer to its original deployed state by discarding local changes or corruption that occurred in the client-side layer data.

This approach is useful because it repairs the virtualized application without requiring a conventional reinstall of the operating system or manual cleanup of the application’s virtual resources. After the layer is reset, it can be activated again so the client receives a clean, functional instance of the application. This is consistent with the Client Management Suite software virtualization model, in which layer lifecycle actions are used to manage the state of virtualized software on managed endpoints. See Broadcom’s IT Management Suite 8.5 documentation and the Broadcom Knowledge Base for product documentation and administrative guidance.

QUESTION NO: 8 - (SIMULATION)

An administrator did NOT install IT Analytics during the installation of IT Management Suite 8.5.

Which four steps should the administrator take to install and configure IT Analytics?

Place the steps on the left in the correct order on the right side of the screen under "Correct Order".

ANSWER: Check the explanation for the answer

Explanation:

Correct order:

1. Use **Symantec Installation Manager (SIM)** to install the **IT Analytics** solution.
2. Open the **IT Analytics Configuration** page/wizard in the Symantec Management Console and configure the IT Analytics database (SQL Server connection and credentials).

3. Configure the **SQL Server Analysis Services (SSAS)** server/instance for IT Analytics so that the IT Analytics cubes can be created and processed.
4. Configure the IT Analytics data processing/refresh schedule (and Reporting Services, if presented by the wizard), then process the cubes and use the IT Analytics reports.

IT Analytics must first be installed through SIM. Its configuration then creates and connects the IT Analytics data warehouse/database, configures Analysis Services for the OLAP cubes, and finally enables the scheduled data loading/cube processing that makes analytics reports usable.

QUESTION NO: 9

Which two (2) items are attributes of a configuration item in IT Management Suite 8.5? (Select two)

A. Resource association

B. Collation

C. View

D. Hierarchy

E. Data class

ANSWER: A E

Explanation:

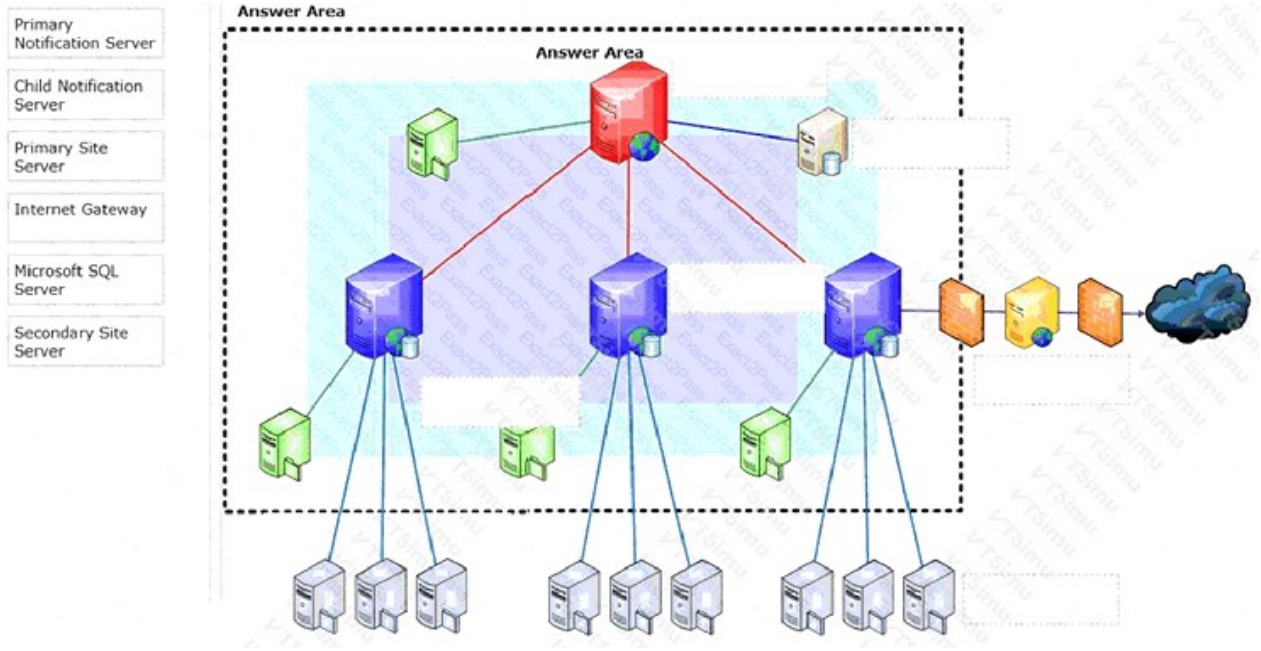
In IT Management Suite, the CMDB represents managed entities as resources and uses configuration items to hold configuration-management information about those resources. **Resource association** is an attribute of a configuration item because it establishes the relationship between the CI and the underlying resource record to which its configuration information belongs. This association enables the CMDB to connect configuration data with the relevant computer, user, software, service, or other managed resource.

Data class is also a configuration-item attribute. A data class defines the structured category of information stored for the CI and the fields that describe it. This provides the CMDB with a consistent, extensible model for recording different types of configuration data while retaining its association with the applicable resource. Together, the resource association and data class identify both the entity represented and the configuration information being maintained for it. Broadcom's IT Management Suite documentation describes the CMDB resource model and the use of data classes for storing resource-related inventory and configuration information. See Broadcom TechDocs: Using CMDB Solution and Broadcom TechDocs: IT Management Suite documentation.

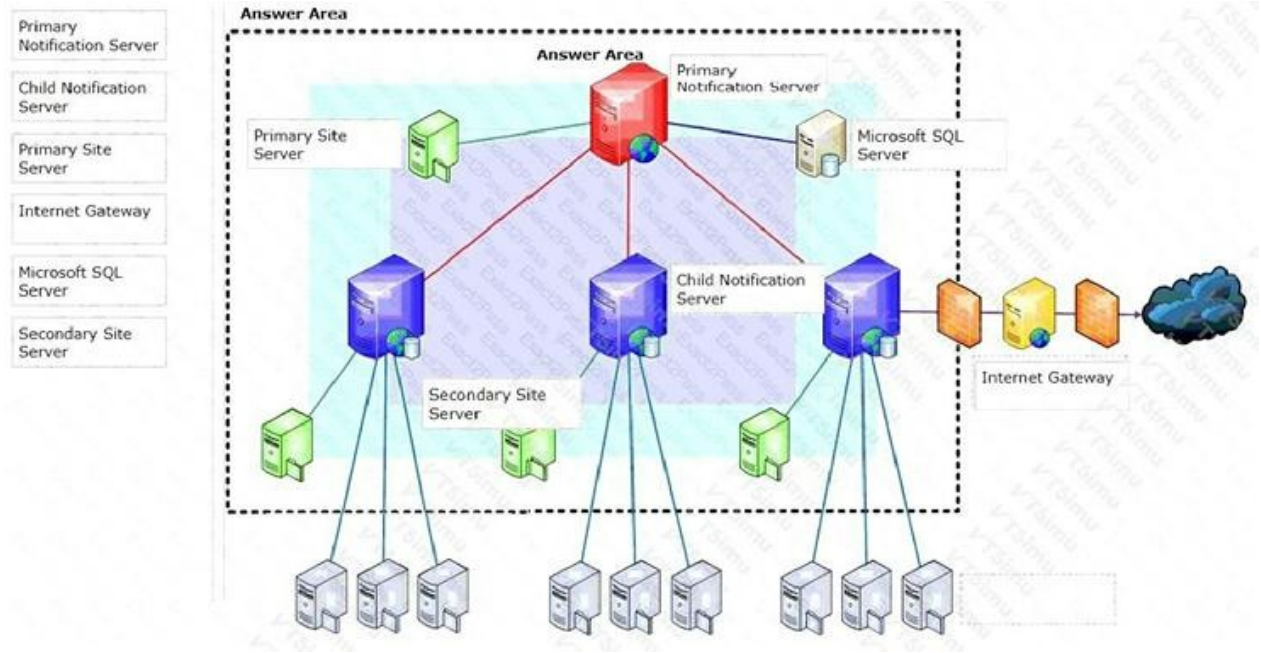
QUESTION NO: 10 - (DRAG DROP)

Where should an administrator place the IT Management Suite 8.5 solution components in this diagram?

Drag and drop the component name to the appropriate component location in the diagram.



ANSWER:



Explanation:

The correct placement follows the standard IT Management Suite hierarchy shown in the diagram. The red server at the top is the **Primary Notification Server**. It is the central management server for the environment and is shown with a globe, reflecting its role as the main Notification Server. The dedicated server at the upper right, shown with the database cylinder, is **Microsoft SQL Server**; this is where the Notification Server environment stores its management data.

The blue servers below the primary tier are **Child Notification Servers**. They extend the Notification Server hierarchy to support managed environments beneath the primary server. The green server directly associated with the primary server is the **Primary Site Server**. It represents the site-server role in the primary site and is positioned on the primary server side of the hierarchy.

The green servers located below and connected to the child notification-server tier are **Secondary Site Servers**. These servers serve the secondary sites under the child Notification Server structure and provide the local distribution and management presence for computers at those sites. The yellow, externally facing server positioned between the firewalls and leading toward the Internet cloud is the **Internet Gateway**. It provides the controlled connection used for internet-based communication with managed devices outside the internal network perimeter.

This arrangement reflects the scalable Symantec management architecture: the primary server and its database form the core, child Notification Servers expand the hierarchy, site servers support local device management, and the Internet Gateway supports externally connected clients. Broadcom's official IT Management Suite documentation provides the product documentation and architecture resources for these server roles.

QUESTION NO: 11

Which two (2) elements can an administrator include when building a resource target in the

Computers blade of the IT Management Views? (Select two.)

A. Resource filters

B. Data classes

C. Resource associations

D. Organizational groups

E. Filter criteria

ANSWER: A E

Explanation:

Resource filters and filter criteria can both be used to define the membership of a resource target in the Computers blade. A resource filter is a reusable, saved definition that identifies managed resources according to an established set of conditions. Including it in a target lets an administrator apply an existing, centrally maintained grouping of computers without recreating its logic. This is particularly useful where the same scope must be consistently used by multiple policies, tasks, reports, or views.

Filter criteria provide the direct, rule-based portion of target construction. The administrator can specify conditions based on inventory and resource properties so that computers are dynamically included when they meet the defined conditions. Consequently, target membership can change automatically as managed computers report updated inventory or their relevant resource data changes. Combining reusable resource filters with directly configured filter criteria gives administrators a flexible way to scope computer management activity while retaining dynamic membership evaluation. Broadcom's Client Management Suite documentation describes management of resource targets and computer resources in the Symantec Management Platform: Client Management Suite 8.5 documentation and Using Client Management Suite.

QUESTION NO: 12

Which two (2) events or methods allow the administrator to create a backup of Notification

Server cryptographic keys? (Select two.)

A. Before the installation of the Symantec Management Platform or subsequent solutions are completed

B. During the first-time installation of the Symantec products

C. After the installation of the Symantec Management Platform or subsequent solutions are completed

D. While in the Symantec Management Console by choosing Settings > All settings > Notification Server Backup

E. In the Symantec Management Console under Home > First time setup

ANSWER: B C

Explanation:

Notification Server cryptographic keys protect sensitive information used by the Symantec Management Platform, including credentials and other encrypted data held within the environment. A key backup can be created during the first-time installation of the Symantec products, when the installation and initial configuration process provides the opportunity to protect the newly created cryptographic material. This establishes a recoverable copy from the outset of a new Notification Server deployment.

An administrator can also create a backup after the installation of the Symantec Management Platform or subsequent solutions are completed. This is important operationally because the key backup process remains available after deployment, allowing administrators to create or refresh protected backup copies as part of normal server-maintenance and disaster-recovery procedures. Keeping the backup accessible, protected by its configured password, and separate from the Notification Server itself helps ensure that encrypted data can be recovered if the server must be rebuilt or restored. Broadcom's IT Management Suite documentation and product documentation portal provide the administrative guidance for managing Notification Server configuration and recovery-related tasks: Broadcom IT Management Suite documentation and Broadcom Knowledge Base.

QUESTION NO: 13

Which action must an administrator perform before an Agentless Inventory can be run against Network Devices?

A. Import resources into the CMDB

B. A Full Inventory on all known systems

C. A Microsoft Active Directory import

D. A Network Discovery Task (Discovery Network)

ANSWER: D

Explanation:

A Network Discovery Task (Discovery Network) must be run first because agentless inventory requires Network Devices to be discovered and represented as managed resource records before inventory collection can target them. The Discovery Network task scans the defined network ranges and identifies reachable devices, gathering the basic identity and connectivity information needed to create those network-device resources in the CMDB. Once these discovered resources exist, an administrator can configure and run an agentless inventory task against the appropriate network-device targets or filters.

This workflow is particularly important for devices that cannot run the Symantec Management Agent, such as switches, routers, printers, and other SNMP-capable infrastructure. Discovery establishes the list of devices and their properties; agentless inventory then queries those devices remotely, typically using the configured network credentials and protocols, to collect the additional inventory data. Broadcom's IT Management Suite documentation describes Network Discovery as the process used to discover network devices and create resource records, and its Inventory Management documentation covers inventory collection from devices that do not have an installed agent. See Broadcom Network Discovery documentation and Broadcom Inventory Management documentation.

QUESTION NO: 14

An administrator needs to reset student lab computers to a fresh state to prepare for the next group of students, when the computers are reset, the operating system a manually installed. The administrator then physical drivers and applications for each unique system one at a time with physical media. The process is inefficient and highly prone to error.

Which two (2) benefits would the organization realize by using Deployment Solution?

(select two).

A. Automated installation of the operating system using a scripted OS installation wizard.

B. Automated installation of the drivers for each system using prepare the image tasks

C. Automated application installations through use of the software portal

D. Automated driver installation using deployanywhere

E. Automated installation of the operating system using pc trasplant

ANSWER: A D

Explanation:

Deployment Solution enables administrators to standardize and automate repeated computer-provisioning work through deployment jobs and tasks. “Automated installation of the operating system using a scripted OS installation wizard” is a direct benefit because a scripted OS installation can apply an operating system consistently to lab computers without requiring the administrator to manually install it at each device. This provides a repeatable baseline for every new student group and reduces the time required to return systems to a known state.

“Automated driver installation using DeployAnywhere” is also a core Deployment Solution benefit. DeployAnywhere injects or installs the appropriate mass-storage and hardware drivers as part of an image deployment, allowing a common operating-system image to be deployed across differing hardware models. This avoids the manual, device-by-device driver installation described in the scenario and makes deployments more reliable and scalable. Together, scripted operating-system deployment and DeployAnywhere address both major sources of manual effort: rebuilding the OS and configuring hardware-specific drivers. Broadcom’s Deployment Solution documentation describes its operating-system deployment and imaging capabilities, including hardware-independent deployment support through DeployAnywhere.

See the Broadcom Deployment Solution 8.5 documentation and the Broadcom Deployment Solution product page.

QUESTION NO: 15

The Symantec agent is currently communicating with the notification server via https.

Which additional prerequisite must be met for the Symantec management agent to communicate over the internet?

A. The agent must have the internet gateway agent plug-in installed on the client.

B. The agent must open a secure tunnel to the notification server

C. The agent must receive a cloud-enabled management settings policy.

D. The agent must receive a targeted agent settings policy.

ANSWER: C

Explanation:

The agent must receive a cloud-enabled management settings policy. Cloud-enabled management is the Symantec Management Agent capability designed to let managed computers continue communicating with the Notification Server when they are outside the internal corporate network. HTTPS communication is a foundational requirement because the agent must use a secure, Internet-accessible Notification Server endpoint. The cloud-enabled management settings policy supplies the agent-side configuration that enables this mode of communication and identifies how the agent should operate when it is connected through the Internet rather than the local management network.

In practice, an administrator enables and configures cloud-enabled management in the Symantec Management Platform and then targets the resulting settings policy to the applicable computers. Once the policy is received, the agent can evaluate its network location and use the configured Internet communication settings to contact the Notification Server securely. This policy-based configuration is important because it centrally controls the behavior of potentially remote clients and allows the environment to apply the intended server and communication settings consistently. Broadcom documents Cloud-enabled Management as part of the IT Management Suite administration and usage documentation: Broadcom TechDocs: IT Management Suite. Product capabilities and documentation resources are also available from the Broadcom IT Management Suite product page.

QUESTION NO: 16

How can an administrator quickly view and export report results while creating a filter based on the location of computers?

A. Executing the Filter Results Report Builder

B. Executing Assets by Location Organizational View Builder

C. Executing and saving the IT Analytics Computers by Location Report Builder

D. Executing the Computers by Location Report Builder

ANSWER: A

Explanation:

Executing the Filter Results Report Builder is correct because this report builder is specifically intended to display the resources returned by a filter. An administrator can use it while defining or working with a location-based filter to immediately inspect the matching computer resources rather than creating a separate, purpose-built reporting object. The resulting grid provides a practical way to validate that the filter identifies the intended computers and to export those displayed results for operational use, such as sharing an inventory list or reviewing location assignments outside the console.

In Symantec Management Platform, filters are dynamic or static resource collections that can be used throughout the console for targeting, reporting, and management tasks. Viewing filter results is therefore the direct workflow when the goal is to see the computers selected by filter criteria. The Filter Results Report Builder connects the filter's selected resources with report-style output and export functionality, making it the fastest fit for the stated requirement. Broadcom's Client Management Suite documentation provides the platform context for resource filtering and reporting features: Client Management Suite 8.5 documentation. Additional product documentation and knowledge resources are available through the Broadcom Knowledge Base.