PassQueen
a.k.a dumpsqueen.com

# A00-250 SAS Platform Administration for SAS9

## SAS Institute A00-250

**Version Demo**

**Total Demo Questions: 10**

**Total Premium Questions: 102**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Managing the SAS Platform | 12 |
| Topic 2, Managing Users | 5 |
| Topic 3, Managing Security | 42 |
| Topic 4, Managing Data | 14 |
| Topic 5, Managing Servers | 22 |
| Topic 6, Monitoring and Troubleshooting | 7 |
| Total | 102 |

QUESTION NO: 1

You used the SAS Add-In for Microsoft Office in Microsoft Excel to view a SAS OLAP cube. Which type of server is used to access the OLAP cube?

**A.** OLAP server

**B.** Workspace server

**C.** OLAP and workspace server

**D.** OLAP and batch server

**ANSWER: A**

**Explanation:**

The correct answer is **OLAP server**. A SAS OLAP cube is a multidimensional data store designed for interactive analysis, including drill-down, roll-up, filtering, and viewing summarized measures by dimensions. When a user opens and analyzes a cube through SAS Add-In for Microsoft Office in Excel, the add-in connects to the SAS OLAP Server that hosts and serves the cube. The OLAP Server handles the multidimensional query requests and returns the aggregated results needed for the Excel analysis view.

In a SAS 9 deployment, the OLAP Server is configured and managed as a server component in SAS metadata and is associated with the cube definitions registered in the SAS Metadata Server. Users must have appropriate metadata-layer permissions to see and query a cube, but the server that provides access to the cube's OLAP content is specifically the OLAP Server. SAS documentation describes SAS OLAP Server as the component that enables users to query and analyze OLAP cubes, while SAS Add-In for Microsoft Office provides a client interface for working with those SAS resources from Microsoft Office applications. See the SAS OLAP Server documentation and the SAS Add-In for Microsoft Office documentation.

**QUESTION NO: 2**

How many object spawners, at a minimum, need to be defined in the metadata?

**A.** One per machine running a stored process server, workspace server, and/or pooled workspace server.

**B.** One for each type of server instantiated byanobject spawner.

**C.** One for every three servers that need to be instantiated by an objectspawner.

**D.** Never more than one per environment.

**ANSWER: A**

**Explanation:**

One per machine running a stored process server, workspace server, and/or pooled workspace server is correct. The SAS Object Spawner is a host-based process: it runs on a particular machine and listens for client connection requests there. When a request arrives, it starts the appropriate SAS server process that is configured in metadata for that host, such as a SAS Workspace Server, SAS Pooled Workspace Server, or SAS Stored Process Server. A single Object Spawner can therefore launch multiple eligible server types on the same physical or virtual machine; it is not necessary to define a separate spawner for each server definition on that machine. However, a spawner running on one host cannot start a server process on another host. Consequently, each machine that hosts one or more of these spawner-managed SAS servers requires its own Object Spawner definition and corresponding running spawner service. This host-level deployment model ensures that metadata connection information directs requests to a local spawner that can create the requested server session. SAS administration documentation describes the Object Spawner as the component that starts SAS servers in response to client requests and provides its configuration through SAS metadata. See the SAS Object Spawner documentation and the SAS documentation portal.

## QUESTION NO: 3

A platform administrator wants to prevent all restricted users from accessing data that requires the Read permission. Which permission level(s) should the platform administrator assign?

**A.** RM and R for PUBLIC

**B.** RM and R for PUBLIC and

**C.** R for PUBLIC

**D.** RM for PUBLIC and SAS

## ANSWER: C

**Explanation:**

**R for PUBLIC** is correct when the Read permission is explicitly denied for the PUBLIC identity. Every authenticated SAS user is an implicit member of PUBLIC, including restricted users. Therefore, setting an explicit denial of Read for PUBLIC prevents those users from reading a protected resource whose access is governed by the Read permission. This approach is especially useful when the goal is to apply a consistent restriction to the entire restricted-user population rather than managing permissions user by user.

In SAS metadata authorization, Read is the permission that governs access to an object's associated content, such as a table or other data resource. A user must have the applicable effective permissions to access that content. An explicit denial assigned through PUBLIC is inherited by all members of PUBLIC and takes precedence in the effective authorization decision, ensuring that restricted users cannot obtain Read access through that broad identity. The administrator should apply this denial only at the appropriate metadata object or folder scope, so that it protects the intended data without unintentionally affecting unrelated resources. SAS documents the permission meanings and the authorization evaluation model in the SAS 9.4 Security Administration Guide and its authorization documentation.

## QUESTION NO: 4

How do you modify the logging levels of a server without having to restart the server?

**A.** Modify theRollingFileAppender.

**B.** Use the IOMServerAppender to specify the message.

**C.** Use the Server Manager plug-in to modify the logger settings dynamically.

**D.** Modify the logconfig.xml file.

## ANSWER: C

**Explanation:**

Use the Server Manager plug-in to modify the logger settings dynamically. In SAS Management Console, the Server Manager plug-in provides administrative access to configured SAS servers and includes a logging facility for supported server types. An administrator can select a server, open its logging configuration, and change the threshold level for an existing logger while that server is running. The change is communicated to the server dynamically, so it takes effect without stopping and restarting the service. This is particularly useful for temporarily increasing diagnostic detail during troubleshooting, then restoring the normal production logging level after the issue has been investigated. Dynamic logger changes apply to the active server process and are intended for operational control of logging at run time. Administrators should have the required authorization to manage the relevant server and should use the server's current logging configuration to identify the logger whose level needs adjustment. SAS documentation describes the Server Manager plug-in's role in managing server logging and dynamic logging-level changes: SAS Management Console: Server Manager. Additional logging administration guidance is available in the SAS Intelligence Platform: Security Administration Guide.

## QUESTION NO: 5

A host is using an LDAP provider as a back-end authentication mechanism. For this setup, how does the SAS server view the authentication?

**A.** integrated authentication

**B.** back-end authentication

**C.** internal authentication

**D.** host authentication

**ANSWER: D**

**Explanation:**

Host authentication is correct. In this arrangement, the SAS server delegates verification of the supplied user ID and password to the host operating system's authentication service. The host, in turn, has been configured to use LDAP as its directory or identity provider. Because LDAP is operating behind the host authentication layer rather than being contacted directly by the SAS server as the server's own authentication provider, SAS categorizes the login as host authentication.

This distinction is important for SAS platform administration: the authentication type describes the mechanism as seen and used by the SAS server, not every identity component that may participate behind the operating system. SAS receives the host-level authentication result and then proceeds with SAS metadata identity and authorization processing for the authenticated user. Thus, LDAP can be the back-end repository used by the host while the SAS server still treats the credential validation path as host authentication. SAS documentation describes host authentication as relying on the operating environment to authenticate users and distinguishes it from authentication mechanisms configured directly for SAS components. See the SAS Documentation portal and the SAS Support documentation library for SAS 9 security and authentication administration guidance.

**QUESTION NO: 6**

A registered SAS library is associated with more than one application server. A platform administrator modifies the library definition in SAS Management Console. What is the result?

**A.** The modified library definition is used by all associated application servers.

**B.** The modification applies only to the server on which SAS Management Console is running.

**C.** A separate copy of the library definition is created for each application server.

**D.** The modification applies only after the library is promoted.

**ANSWER: A**

**Explanation:**

**The modified library definition is used by all associated application servers.** A library definition is a single metadata object that can be associated with multiple application-server contexts. Changes to common properties in that metadata definition, such as the engine, physical path, or connection information, affect the library wherever that same definition is assigned.

If different connection properties are required for separate server contexts, separate library definitions are generally needed. See the SAS 9.4 Intelligence Platform: System Administration Guide.

**QUESTION NO: 7**

A platform administrator changes the physical path of a BASE engine library that is registered in metadata. Which action is required for clients to use the new location?

**A.** Update the library definition in SAS metadata.

**B.** Run PROC METALIB against the library.

**C.** Restart the SAS Metadata Server.

**D.** Recreate the foundation repository.

**ANSWER: A**

**Explanation:**

The administrator must **update the library definition in SAS metadata**. The physical path is part of the library metadata definition. Metadata-aware clients use that definition when they assign the library, so the registered path must match the new physical location.

Moving the directory at the operating-system level does not automatically update the metadata definition. After the library properties are updated, the administrator should validate that the relevant server identity has the required operating-system permissions for the new path. See the SAS Documentation portal for SAS library administration information.

## QUESTION NO: 8

An identity hierarchy specifies a list of identities and the order of precedence of those identities. Which listing of identities is ranked from highest priority to lowest priority?

**A.** User, direct group, indirect group, SASUSERS, PUBLIC

**B.** User, SASUSERS, PUBLIC, directgroup, indirect group

**C.** SASUSERS, PUBLIC, User, direct group, indirect group

**D.** direct group, indirect group, User, PUBLIC, SASUSERS

**ANSWER: A**

**Explanation:**

The correct identity hierarchy is **User, direct group, indirect group, SASUSERS, PUBLIC**. In SAS metadata authorization, permissions can be assigned to an individual user or to groups to which that user belongs. When permissions from multiple identities must be evaluated, SAS uses identity precedence to determine how the identities are considered. The individual user identity has the highest priority because it is the most specific identity. Next come groups in which the user is a direct member, followed by indirectly inherited group memberships, reflecting the nesting relationship of the groups. The built-in SASUSERS group is evaluated after user-defined direct and indirect group memberships. Finally, PUBLIC has the lowest priority because it represents all users, including users who do not have an individual metadata identity. Understanding this hierarchy is important when administering access controls, especially when permissions are assigned at different levels of specificity. Administrators can use the effective-permissions tools in SAS Management Console to inspect the identities and authorization decisions that apply to a user. SAS documentation describes identity precedence and its role in the metadata authorization process: SAS 9.4 Intelligence Platform: Security Administration Guide. See also the SAS documentation portal at documentation.sas.com.

## QUESTION NO: 9

Which statement regarding default groups is true?

**A.** SASUSERS is a subset of PUBLIC

**B.** PUBLIC is a subset of SASUSERS

**C.** SASUSERS is a subset of ADMINISTRATORS

**D.** ADMINISTRATORS is a subset of Unrestricted Users

**ANSWER: A**

**Explanation:**

**SASUSERS is a subset of PUBLIC** is correct. In SAS metadata security, SASUSERS and PUBLIC are implicit default groups that help establish a baseline for authorization. SASUSERS represents all users who have an authenticated identity in the SAS Metadata Server. PUBLIC is broader: it includes the SASUSERS group and can also represent access that is available generally, including to users who are not individually registered in metadata where the applicable SAS environment and authentication configuration permit it. Therefore, every authenticated user represented through SASUSERS is also included through PUBLIC, making SASUSERS a subset of PUBLIC.

This relationship matters when assigning permissions in SAS Management Console. An authorization grant made to PUBLIC can apply very broadly, including to all authenticated SAS users through their SASUSERS membership. Administrators should account for this inherited group relationship when evaluating effective permissions, particularly for shared metadata objects, folders, stored processes, and application capabilities. SAS documents these default and implicit groups as part of its metadata authorization model; their membership is system-defined rather than maintained as ordinary, manually managed group membership. See the SAS 9.4 Security Administration Guide and the SAS documentation portal.

**QUESTION NO: 10**

The suffix of a SAS Internal account is:

**A.** @sas

**B.** @saspw

**C.** @LocalHost

**D.** @sasMain

**ANSWER: B**

**Explanation:**

**@saspw** is the suffix used for a SAS internal account in SAS 9. A SAS internal account is stored and authenticated in the SAS metadata server rather than by an external identity provider such as an operating-system account, LDAP directory, or Active Directory domain. SAS identifies these accounts using a qualified user ID in the form `userID@saspw`. For example, the predefined unrestricted administrative account is commonly represented as `sasadm@saspw`. The suffix is important because it tells SAS that the credentials are to be validated against the metadata server's internal authentication domain. Administrators use SAS internal accounts for specific administrative and service purposes, particularly when an external authentication source is unavailable or when a dedicated metadata-based identity is required. The account's password and related authentication information are managed through SAS metadata administration tools and processes. SAS documentation describes SAS internal accounts as accounts whose user IDs end in `@saspw`, including the predefined `sasadm@saspw` administrator account. See the SAS 9.4 security administration documentation and the SAS Intelligence Platform security guide.