PassQueen
a.k.a dumpsqueen.com

SolarWinds Observability Self-Hosted Fundamentals

SolarWinds Observability-Self-Hosted-Fundamentals

Version Demo

Total Demo Questions: 9

Total Premium Questions: 91

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which two of the following statements apply to SolarWinds Hybrid Cloud Observability (HCO) Platform? (Choose two.)

A. can operate without an internet connection

B. can be deployed on-premises or in the cloud

C. provides AIOps and machine learning technology

D. requires SolarWinds hybrid cloud observability

ANSWER: A B

Explanation:

SolarWinds Hybrid Cloud Observability is a self-hosted monitoring platform, so its principal monitoring components—including polling engines, the SolarWinds Platform server, databases, alerting, reporting, and web access—run within infrastructure controlled by the organization. Consequently, it can operate without an ongoing public internet connection. Internet connectivity can be useful for activities such as obtaining installers, product updates, online licensing workflows, and optional connected services, but it is not required for the platform's core collection and monitoring operations after deployment. SolarWinds also supports installing the platform on physical or virtual infrastructure in an organization's data center and supports deployment in public-cloud infrastructure. This flexibility lets teams locate the monitoring system where it best meets their operational, security, network-access, and data-residency requirements while monitoring both on-premises and cloud-hosted environments. SolarWinds describes Hybrid Cloud Observability as self-hosted and designed to provide unified visibility across hybrid IT environments. The SolarWinds Platform installation documentation also details requirements and supported deployment planning for the self-hosted platform. See the Hybrid Cloud Observability introduction and the SolarWinds Platform Installation Guide.

QUESTION NO: 2

Which three of the following user accesses are available when restricting access to reports on SolarWinds Hybrid Cloud Observability (HCO)? (Choose three.)

A. standard users can be prevented from accessing all reports

B. standard users can be prevented from accessing reports by other users

C. standard users can be prevented from accessing the report manager

D. standard users can be prevented from accessing their reports

ANSWER: A B C

Explanation:

SolarWinds Hybrid Cloud Observability Self-Hosted uses SolarWinds Platform account permissions and report limitations to control what standard users can do in the reporting area. **standard users can be prevented from accessing all reports** because an administrator can configure the account so that reports are unavailable to that user. This is appropriate when a user does not need reporting functionality at all.

standard users can be prevented from accessing reports by other users because report limitations can constrain report visibility to a user's own reports and, where configured, reports shared with that user. This allows teams to protect report definitions and output that may contain operational or business-sensitive information while still allowing users to work with authorized reports.

standard users can be prevented from accessing the report manager because access to report-management functions is separately controlled from basic report viewing. Administrators can therefore limit a standard account to consuming permitted reports without granting the management capabilities used to create, modify, schedule, or administer reporting

content. These controls support least-privilege access and should be assigned according to each user's reporting responsibilities. See SolarWinds guidance on user account permissions and the SolarWinds Platform reporting feature.

QUESTION NO: 3

Which two of the following platforms is supported by the agent software? (Choose two.)

A. Debian 11

B. Fedora Linux

C. Windows 11 Enterprise

D. Windows Server 2022

ANSWER: C D

Explanation:

Windows 11 Enterprise and Windows Server 2022 are supported platforms for deployment of the SolarWinds Platform Agent. The Windows agent is installed locally on a monitored node and enables the SolarWinds Platform to collect status, performance, and other monitoring data without requiring all polling to originate remotely. SolarWinds documents support for current Windows client and server operating systems, including the Enterprise edition of Windows 11 and Windows Server 2022. This makes the agent appropriate for both enterprise workstations and modern server workloads when agent-based monitoring is needed, such as for nodes behind firewalls, in remote networks, or where WMI/SNMP polling is not the preferred collection method.

Operating-system support must be verified against the agent requirements for the installed SolarWinds Platform version, because supported versions and feature availability can change over time. The authoritative requirements also distinguish supported Windows releases from the separately documented Linux-agent distributions and installation prerequisites. See the SolarWinds documentation for SolarWinds Platform Agent requirements and the SolarWinds Platform product requirements.

QUESTION NO: 4

An administrator is investigating a business application that is reported as slow. The administrator needs to view the application together with dependent servers, databases, and infrastructure components to determine where the issue may be occurring. Which tool should be used first?

A. Alert Manager

B. AppStack

C. PerfStack

D. Report Manager

ANSWER: B

Explanation:

AppStack is the appropriate starting point because it provides an application-centric view of monitored entities and their discovered relationships. It helps an administrator see the affected application in the context of dependent infrastructure and identify components that may be contributing to the service issue.

PerfStack is used to correlate selected time-series metrics across entities. It is useful after the relevant entities and metrics have been identified, but it does not provide the same dependency-oriented application-stack view.

QUESTION NO: 5

An alert has several escalation levels configured to notify different teams if a condition remains active. An operator acknowledges the alert shortly after it triggers. Which two statements are accurate? (Choose two.)

A. Further alert escalation is halted.

B. The underlying alert condition can remain active.

C. The alert is immediately reset regardless of its reset condition.

D. The monitored object is automatically changed to unmanaged.

ANSWER: A B

Explanation:

Further alert escalation is halted and **the underlying alert condition can remain active**. Acknowledgement records that the alert has been seen and stops subsequent escalation actions for that active alert instance. It does not resolve the monitored issue or force the alert to reset.

The alert resets only when its reset condition is met. Acknowledgement also does not change the monitored object's polling method or suppress unrelated alerts.

QUESTION NO: 6

A user indicates when a map is created, only entities can be seen and status is not available. In addition, maps are unable to be nested. What is causing this issue?

A. user account doesn't have administrative rights

B. user account doesn't have map editing rights

C. user account doesn't have node management rights

D. user account doesn't have view edit rights

ANSWER: B

Explanation:

The user account doesn't have map editing rights. In SolarWinds Observability Self-Hosted, map-related permissions determine whether an account can use the full map-management experience rather than only a restricted representation of monitored entities. Map editing access is required for creating and modifying maps and for using map-management features such as organizing map content into a hierarchy by nesting maps. This permission also enables access to the map information and selectable object details needed to work with entity status in the map editor. An account without those rights may be able to view entities that are available through its existing object limitations, but it cannot fully configure map behavior or structure. An administrator should edit the account and grant the applicable Map Management or map-editing permission, while retaining appropriate node and object limitations for the user’s role. SolarWinds documents account permissions and limitations in its Manage accounts documentation. For the map feature and its management capabilities, see the SolarWinds Maps documentation.

QUESTION NO: 7

What is the effect of checking the Encrypt connections with SSL box in the configuration wizard?

A. The installed SolarWinds product will use the login account to access the databases on theSQL server.

B. The login account to access the SQL server will be encrypted and stored in SolarWinds'Hybrid Cloud Observability Platform server.

C. The login credentials will be encrypted between SolarWinds' Hybrid Cloud ObservabilityPlatform server and the SQL server while in transit.

D. The network data between SolarWinds' Hybrid Cloud Observability Platform server and theSQL server will be encrypted.

ANSWER: D

Explanation:

Checking **Encrypt connections with SSL** causes the SolarWinds Platform server to use an encrypted connection when communicating with the SQL Server database. Therefore, **The network data between SolarWinds' Hybrid Cloud Observability Platform server and the SQL server will be encrypted.** This protection applies to the database communication channel, safeguarding data in transit between the application server and SQL Server rather than only protecting a particular credential or a single authentication exchange.

SolarWinds Platform products depend on SQL Server for operational, configuration, and monitoring data. Encrypting the SQL connection helps preserve the confidentiality and integrity of that traffic if it traverses network segments where interception is a concern. The setting corresponds to SQL Server transport encryption, which uses TLS to protect the client-server session. For a secure deployment, SQL Server must be appropriately configured for TLS and the SolarWinds server must be able to validate the SQL Server certificate. SolarWinds documents database connection settings as part of Configuration Wizard workflows, and Microsoft describes how SQL Server encryption protects communications between clients and the database engine.

See the SolarWinds Platform Configuration Wizard documentation and Microsoft guidance for enabling encrypted SQL Server connections.

QUESTION NO: 8

Platform administrators are to be given access to view all reports created and used in SolarWinds Hybrid Cloud Observability (HCO), regardless of who created them or their permission settings. Which report limitation setting should be used?

A. default

B. new limitation

C. no limitation

D. no reports

ANSWER: C

Explanation:

no limitation is the appropriate report limitation setting because it gives the account unrestricted access to reports in the SolarWinds Platform. This is appropriate for platform administrators who must be able to view reports across the environment, including reports created by other users and reports that may otherwise be scoped through account limitations or report permissions. SolarWinds account-management permissions can be combined with limitations to control what a user can access; assigning no limitation for reports ensures that report visibility is not narrowed by an account-specific report scope. This supports centralized administration, troubleshooting, auditing, and report maintenance, since administrators can locate and review reports regardless of their creator or intended audience. The setting should be applied to an account with the necessary administrative and reporting permissions so that unrestricted report scope can be used for legitimate platform-management duties. See SolarWinds guidance on accounts and permissions and the account limitations documentation for the relationship between permissions, limitations, and accessible objects.

QUESTION NO: 9

Which out-of-the-box property is associated with a web-based report?

A. category

B. creator

C. format

D. owner

ANSWER: A

Explanation:

category is the out-of-the-box property associated with a web-based report. SolarWinds Observability Self-Hosted uses report categories to organize report definitions in Report Manager, allowing administrators and users to browse related reports together and locate the reports relevant to a particular operational area. Built-in reports are supplied within categories, and a report created through the web console is assigned to a category as part of its definition. This classification is therefore persistent metadata for the report itself, rather than a temporary setting applied only when the report is viewed, exported, or delivered.

Categories also support practical report management as deployments grow: teams can group reporting content by monitoring domain, operational purpose, or organizational convention, and the Report Manager navigation presents reports according to that structure. SolarWinds documentation describes managing reports through the web console and organizing report content in Report Manager, including the use of categories when creating and maintaining reports. See the SolarWinds Platform documentation for managing reports and the documentation for creating reports.