TESTPASSPORT

PRACTICE QUESTIONS

High Quality | Better Service

Exam : **Observability Self Hosted Fundamentals**

Title : SolarWinds Observability Self-Hosted Fundamentals

Version : DEMO

1.A performance issue on a network is being troubleshooted and needs customization of metrics and entities to be viewed during troubleshooting.
Which tool combination / no combination would allow this to happen?
A. AppStack allows customization of entities and PerfStack allows customization of metrics
B. AppStack alone allows customization of metrics and entities
C. AppStack and PerfStack combined together allow customization of metrics and entities
D. PerfStack alone allows customization of metrics and entities
Answer: A
Explanation:
The SolarWinds Platform provides distinct tools for visualizing different aspects of environmental health and performance. AppStack is primarily an entity-relationship mapping tool. According to the SolarWinds SAM Administrator Guide, "The AppStack Environment view provides a powerful layer of troubleshooting visibility by exposing all participating objects in your environment, as well as their relationships to one another". It allows administrators to customize which entities (nodes, applications, volumes, etc.) are visible and how they are grouped to show dependencies.
Conversely, PerfStack (Performance Analysis) is the engine used for metric correlation. As stated in the SolarWinds Platform Administrator Guide, PerfStack allows users to "drag and drop performance metrics from multiple entities onto a single chart to correlate data over time". While AppStack excels at showing what is connected, PerfStack excels at showing how specific metrics (CPU, Latency, IOPS) across those connected entities interact. Therefore, a combination is required where AppStack handles the entities and PerfStack handles the metrics. Specifically, you use AppStack to identify the scope of entities involved in a performance bottleneck and then transition those entities into a PerfStack project to perform a deep-dive analysis of the metrics. This modular approach ensures that troubleshooting is both contextually aware (via AppStack) and data-driven (via PerfStack).

2.How can access to all reports be removed from user accounts?
A. add to report group and modify access
B. disable manage reports permissions
C. set user account report limitation to default
D. set user account report limitation to no reports
Answer: D
Explanation:
In the SolarWinds Platform, report access is governed by both functional permissions and account limitations. While "Disable Manage Reports" (Option B) prevents a user from editing or creating reports, it does not necessarily hide the "Reports" menu or prevent the user from viewing existing reports they have access to. To completely remove the visibility and accessibility of all reports for a specific user account, an Account Limitation must be applied.
According to the SolarWinds Platform User Account Management documentation, account limitations act as a security filter that restricts what the user can see throughout the entire Web Console. By navigating to Settings > All Settings > Manage Accounts, selecting the user, and editing their Report Limitation, an administrator can choose "No Reports". This configuration ensures that when the user logs in, the Reports section will either be empty or completely hidden from their navigation bar, regardless of their other permissions. This is the most effective method for high-security environments or multi-tenant deployments where certain users should have zero visibility into the historical performance data or

inventory summaries contained within the reporting engine.

3.What indicates an alert cluster has been eliminated (i.e., end conditions have been met)?
A. auto-closed
B. closed
C. completed
D. resolved
Answer: A
Explanation:
In Hybrid Cloud Observability (HCO), specifically within the AlertStack feature, related alerts are grouped into clusters to reduce "alert fatigue" and provide a unified view of an incident. According to the SolarWinds HCO Alerting Guide, an alert cluster transitions through several states based on the status of the underlying trigger conditions.
When the primary issues that triggered the alerts within the cluster are addressed and the "Reset Conditions" for those alerts are satisfied, the cluster is automatically managed by the system. The term used to define a cluster that has met its end conditions is auto-closed. Unlike manual "acknowledgment" or "resolution," which are user-driven actions, "auto-closed" signifies that the platform's monitoring engine has verified the environment has returned to a healthy state and the cluster no longer requires active monitoring or intervention. This automated lifecycle management is central to the AIOps and machine-learning capabilities of the platform, ensuring that the dashboard only reflects currently active, actionable incidents rather than historical events that have already been naturally corrected.

4.What are custom properties and how are they used?
A. built-in attributes used for dynamic device grouping
B. static fields used to identify nodes in SQL database
C. static, pre-defined fields automatically applied to all monitored nodes
D. user-defined fields to store additional node or element information
Answer: D
Explanation:
Custom Properties are one of the most versatile features of the SolarWinds Platform, providing a way to extend the metadata associated with monitored objects. The SolarWinds Platform Administrator Guide defines them as "user-defined fields that allow you to add custom information to nodes, interfaces, volumes, or other monitored entities".
Unlike built-in attributes like "IP Address" or "Vendor," which are discovered automatically, custom properties are created by the administrator to suit specific business needs. Common examples include "Site Location," "Emergency Contact," "Department," or "Service Level Agreement (SLA) Tier".
These fields are critical for organization and automation because they allow for:
Filtering and Grouping: You can create groups that automatically include any node where the "Department" custom property is set to "Finance".
Alerting: You can configure alerts to only trigger for nodes marked as "Mission Critical" in a custom property field.
Reporting: Reports can be generated to show the uptime of all nodes belonging to a specific "Owner" or "Cost Center".
Because they are user-defined, they provide the necessary flexibility to map technical monitoring data to

real-world business structures.

5.Which two of the following account types are supported in SolarWinds Hybrid Cloud Observability (HCO)? (Choose two.)
A. Azure active directory (AD)
B. Orion group
C. Windows distribution AD
D. Windows local domain
Answer: A, B
Explanation:
SolarWinds Hybrid Cloud Observability supports a variety of authentication methods to ensure seamless integration with enterprise identity providers. According to the SolarWinds Platform Installation and Upgrade Guide, the two primary modern account types used for centralized management are Azure Active Directory (AD) and Orion Groups.
Azure Active Directory (AD): This allows organizations to leverage their cloud-based identity provider for Single Sign-On (SSO) and centralized user management. HCO integrates directly with Azure AD to authenticate users based on their existing cloud credentials.
Orion Group: This is a local platform account type that allows administrators to define permissions at a group level rather than for individual users. By creating an Orion Group, you can assign a specific set of view, alert, and report permissions once, and any user assigned to that group automatically inherits those rights.
While "Windows Local Domain" (standard AD) is supported for on-premises deployments, the specific phrasing in HCO documentation emphasizes the shift toward cloud-native and group-based management. "Windows distribution AD" is incorrect because SolarWinds requires security groups for permission mapping, not distribution groups.