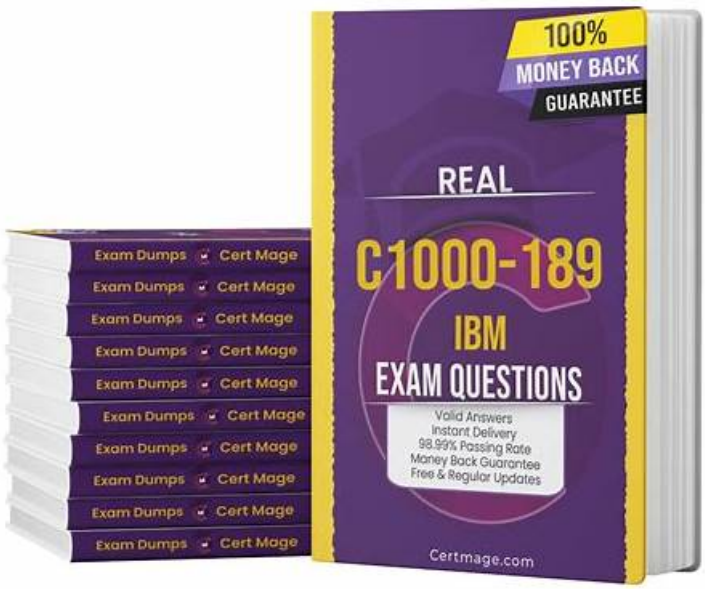
Valid C1000-189 Exam Questions - Examcollection C1000-189 Dumps



P.S. Free & New C1000-189 dumps are available on Google Drive shared by GetValidTest: https://drive.google.com/open?id=1um5orLsvyVIaKPdWKB38GAb5uxQDQ8H-

Do you always feel that your gains are not proportional to your efforts without valid C1000-189 study torrent? Do you feel that you always suffer from procrastination and cannot make full use of your sporadic time? If your answer is absolutely yes, then we would like to suggest you to try our C1000-189 Training Materials, which are high quality and efficiency test tools. Your success is 100% ensured to pass the C1000-189 exam and acquire the dreaming C1000-189 certification which will enable you to reach for more opportunities to higher incomes or better enterprises.

IBM C1000-189 Exam Syllabus Topics:

Topic	Details
Topic 1	• Installation: This section of the exam measures the skills of System Implementation Specialists and focuses on installing and deploying Instana across different environments. It includes installing the Instana backend, deploying and configuring agents, and migrating existing Instana setups. Candidates will also demonstrate their ability to implement Synthetic Monitoring and manage Points of Presence (PoPs) effectively for end-to-end performance validation.
Topic 2	• Troubleshooting: This section of the exam measures the skills of System Support Engineers and focuses on resolving technical and operational issues in Instana. It includes configuring log levels, collecting logs for debugging, and identifying connectivity issues between agents and the backend. Candidates will troubleshoot installation failures, diagnose communication problems, and apply corrective measures to ensure consistent Instana performance and stability across environments.

Topic 3	• Planning: This section of the exam measures the skills of Cloud Monitoring Engineers and covers the foundational planning tasks required for successful Instana deployment. Candidates must understand the installation prerequisites, the architectural design of Instana for on-premises environments, and the platform core capabilities and use cases. It also assesses knowledge of different agent modes, supported sensors and tracers, and the distinctions between cloud service agents and serverless agents essential for scalable implementation.
Topic 4	• Security and Compliance: This section of the exam measures the skills of IT Security Analysts and focuses on the data protection and compliance aspects of Instana deployment. Candidates must describe and implement data retention policies, plan for regulatory compliance, secure APIs, manage user access, and interpret audit logs. The goal is to ensure secure system configurations that align with organizational and regulatory standards.

Examcollection C1000-189 Dumps, Valid C1000-189 Exam Format

Our company has spent more than 10 years on compiling C1000-189 study materials for the exam in this field, and now we are delighted to be here to share our C1000-189 learnign guide with all of the candidates for the exam in this field. There are so many striking points of our C1000-189 Preparation exam. If you want to have a better understanding of our C1000-189 exam braindumps, just come and have a try!

IBM Instana Observability v1.0.277 Administrator - Professional Sample Questions (Q49-Q54):

NEW QUESTION # 49
At which level can AWS agent polling intervals for CloudWatch API be configured?

- A. Service
- B. Region
- C. Account
- D. Resource group

Answer: B

Explanation:
AWS monitoring through Instana involves integration with the CloudWatch API to retrieve platform and service metrics. The official IBM Instana Observability documentation affirms that polling intervals for CloudWatch can be set at the Region level. This means an administrator configures how frequently Instana's agent queries CloudWatch within each specified region independently. This level of granularity provides flexibility: for example, mission-critical regions may be monitored more frequently, while others are polled less often to reduce API costs or remain within AWS rate limits. The documentation specifies: "Instana Agents for AWS can be configured with a polling interval for CloudWatch that is set per Region to customize granularity and resource consumption." Polling cannot be set at the account, resource group, or individual service level in default configuration. Instana's region-based polling helps balance data accuracy and overhead, especially in global or multi-region deployments. If needed, changes are applied through YAML configuration or UI during AWS agent integration setup.

NEW QUESTION # 50
What is required for automatic backend correlation to work given that the EUM agent has been properly set up?

- A. Matching application perspective
- B. Valid HTTPS connection
- C. The Instana SDK
- D. Exposure of the backend trace id

Answer: D

Explanation:
To successfully achieve automatic correlation between frontend and backend traces, Instana requires backend services to expose a trace identity. The IBM Instana EUM and tracing correlation section confirms: "Automatic backend correlation requires exposure and propagation of the backend trace ID to connect user interaction traces with backend processing traces." When the EUM agent operates in browsers or mobile interfaces, it injects headers containing Trace and Span IDs into subsequent backend HTTP requests. Backend instrumentation must read and propagate these identifiers through service calls so Instana can unify them into a single end-to-end transaction trace. Proper correlation connects a user's session-to-service journey across web, application, and infrastructure layers, a fundamental aspect of Instana's distributed tracing model. Lacking backend trace ID propagation causes separated traces that cannot be linked, even if HTTPS, SDK, or application perspectives are configured correctly. This mechanism remains fully verified in the IBM Instana Observability Tracing Integration Guide.

NEW QUESTION # 51
What prevents Ansible actions from manual deletion within Instana?

- A. Default Actions cannot be deleted.
- B. Actions have been imported.
- C. The action is active.
- D. There is no name specified on the action.

Answer: A

Explanation:
IBM Instana documentation is explicit: some action definitions, including default and built-in (such as Ansible) actions supplied by the platform, cannot be manually deleted by users or admins. It states: "Default Actions-including Ansible integration actions pre-defined by Instana-are protected from manual deletion to ensure availability and platform integrity." This ensures that core automation integrations remain functional and the baseline for remediations, regardless of user error or misconfiguration. Custom or imported actions can be removed, but defaults-tagged as such in the UI-are non-removable, safeguarding operational continuity and maintaining standardized integrations across manual and automated workflows. Active status or name presence does not impact deletion ability; it is the default/built-in status (D) that enforces this lock.

NEW QUESTION # 52
Which items are examples of event types that can be used when creating a new alert in Instana?

- A. Logs, Resources, Tracing
- B. Incidents, Offline, Changes
- C. Request, Response, Interruption
- D. Timer, Counter, Level

Answer: B

Explanation:
According to the IBM Instana Observability documentation, event types form the foundation of Instana's alerting system. When configuring new alerts, users can select event categories such as Incidents, Offline, or Changes. The documentation specifies: "Instana alerts are triggered by event conditions derived from incidents (performance degradations), offline detections (component unavailability), and changes (deployment or configuration actions)." Incidents indicate performance or reliability degradation impacting users, Offline events represent disconnected sensors or hosts, while Changes capture deployments or configuration modifications influencing performance. Combining these event types enables contextual alerts and reduces noise by differentiating between symptoms and root causes. Other listed options refer either to data processing concepts (Timers, Counters) or monitoring inputs (Requests, Tracing), not supported as Instana alert event types. These verified categories are consistent across versions 1.0.277 through 1.0.307.

NEW QUESTION # 53
Which logging framework is used by Instana agents?

- A. Loggly
- B. Serilog
- C. Log4j2

- D. JSNLog

Answer: C

Explanation:
IBM Instana Observability agents use Log4j2 as their primary logging framework for system activity, sensor status, and diagnostic output. The documentation confirms: "The default logging framework for Instana agents is Apache Log4j2, providing structured log output, multi-level verbosity, and integration with most enterprise log aggregation environments." Log4j2 is a standard for Java-based environments, supporting dynamic log rotation, filtering, and formatting. Instana agent log files follow Log4j2 conventions, enabling easy parsing by SIEM tools and adapters. Serilog (A) is a .NET framework, not used by Instana agents. JSNLog (C) is for JavaScript applications, while Loggly (D) is a SaaS log analytics platform. Log4j2's mature design lets administrators tune performance, verbosity, and log destinations in rich deployment scenarios, directly aligning with best practices in Instana's monitoring ecosystem. This was reconfirmed in agent reference guides and environment setup sections.

NEW QUESTION # 54
......

What's more, part of that GetValidTest C1000-189 dumps now are free: https://drive.google.com/open?id=1um5orLsvyVIaKPdWKB38GAb5uxQDQ8H-