Latest C1000-189 Braindumps - New C1000-189 Exam Notes

What's more, part of that DumpTorrent C1000-189 dumps now are free: https://drive.google.com/open?id=1Np00OmezY2FVbaUYu8wbTElws2BK_PSy

IBM C1000-189 valid exam simulations file can help you clear exam and regain confidence. Every year there are thousands of candidates choosing our products and obtain certifications so that our IBM Instana Observability v1.0.277 Administrator - Professional C1000-189 valid exam simulations file is famous for its high passing-rate in this field. If you want to pass exam one-shot, you shouldn't miss our files.

IBM C1000-189 Exam Syllabus Topics:

Topic	Details
Topic 1	• Configuration: This section of the exam measures the skills of DevOps Administrators and evaluates their ability to configure and optimize Instana operational settings. It involves setting up business process monitoring, configuring both cloud and serverless agents, and defining agent proxy parameters. Candidates will learn to implement various technologies and sensors, manage OpenTelemetry integrations, set up smart alerts, create service naming rules, and define custom SLIs and payloads for alert channels. Managing licenses and ensuring proper configuration of alerts and notifications are also key components of this domain.
Topic 2	• Integration: This section of the exam measures the skills of Integration Engineers and assesses their proficiency in connecting Instana with external monitoring and automation tools. Candidates must demonstrate knowledge of integrating agent-based systems such as Omegamon, ITM, and ITCAM, as well as external platforms like Prometheus and Grafana. The section also includes configuring alert channels, automation actions, and utilizing the Instana REST API to support customized workflows and data visibility.
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	• 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 5	• 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.

>> Latest C1000-189 Braindumps <<

2026 IBM C1000-189: IBM Instana Observability v1.0.277 Administrator - Professional –Professional Latest Braindumps

By unremitting effort to improve the accuracy and being studious of the C1000-189 real questions all these years, our experts remain unpretentious attitude towards our C1000-189 practice materials all the time. They are unsuspecting experts who you can count on. Without unintelligible content within our C1000-189 Study Tool, all questions of the exam are based on their professional experience in this industry. Besides, they made three versions for your reference, the PDF, APP and Online software version.

IBM Instana Observability v1.0.277 Administrator - Professional Sample Questions (Q36-Q41):

NEW QUESTION # 36
Which action is required to enable features in the Instana Self-Hosted Custom Edition?

- A. Restart the backend.
- B. Modify the deployment settings.
- C. Add feature flags in the configuration file for the core.
- D. Add feature flags in the configuration file for the units.

Answer: C

Explanation:
Enabling advanced features in Instana Self-Hosted Custom Edition requires administrators to add or adjust feature flags in the core configuration file, as per IBM's setup documentation. Specifically: "Feature enablement in Instana Self-Hosted Custom Edition is controlled via feature flags set in the core configuration file, allowing platform-wide updates at startup." Modifying deployment settings may affect resources or endpoints but does not toggle internal features. Unit-level configuration affects only specific microservices, not centralized capabilities. Restarting the backend is necessary after changing configuration but is not itself a feature-enabling action. The central core configuration file, located under the main configuration directory, contains comprehensive toggles for features spanning UI, backend, and data processing pipelines. Only changes made here and saved with appropriate syntax will activate platform features on next start or reload.

NEW QUESTION # 37
What are the two SLI types Instana supports while configuring the service level objectives?

- A. Traces based
- B. Event count based
- C. Alerts based
- D. Error logs based
- E. Time based

Answer: A,B

Explanation:
IBM Instana's Service Level Indicator (SLI) configuration capabilities emphasize trace-based and event count-based SLIs. The verified guide details: "Instana supports SLI definitions based on distributed trace data and event counts, such as request rate, error rate, or latency." Trace-based SLIs allow direct measurement of real user or synthetic transactions for detailed performance objectives (e.g., 99th percentile response time). Event count-based SLIs track operational markers such as number of errors, alerts, or specific incidents-essential for regulatory uptime or compliance audits. Error logs, time-based or alert-based SLIs can be

visualized but are not supported as direct SLI definitions by Instana, according to verified IBM configuration steps. The combination of traces and event counts provides the flexibility to set quality objectives, measure reliability, and drive alerting in line with SRE principles.

NEW QUESTION # 38
What is Instana's custom built software that is designed to monitor a specified technology?

- A. Sensor
- B. Tracer
- C. Profiling
- D. Service

Answer: A

Explanation:
Instana uses Sensors as specialized software components embedded within its agents to monitor and extract telemetry from various supported technologies. The verified documentation states: "Sensors are built-in modules that detect, identify, and monitor specific technologies such as databases, servers, run-times, and messaging systems." These components ensure that the agent collects targeted metrics, events, and traces optimized for individual stacks like MySQL, Kafka, or Java. When deployed, the Instana agent automatically discovers technologies running in the environment and loads corresponding Sensors dynamically, requiring minimal user configuration. Tracers handle transaction propagation, Profiling covers code-level performance, and Service is a higher abstraction in application topology-not individual monitoring logic. The Sensor concept remains core to Instana's automatic discovery and observability architecture as validated in IBM's architectural reference sections.

NEW QUESTION # 39
By default, which rate limit is applied to Instana API calls for per hour usage?

- A. 5,000
- B. 1,000
- C. 6,000
- D. 10,000

Answer: A

Explanation:
Instana sets API rate limits to ensure fair resource usage and platform stability across accounts. According to the IBM Instana Observability documentation, "The default rate limit for the Instana REST API is 5,000 calls per hour per account." This policy is enforced automatically; when an account's API activity reaches the limit, further requests are temporarily blocked until the next hour begins. This guards against accidental overload as well as malicious consumption, and is fundamental for multi-tenant operation. Organizations may request increases for large-scale use cases, but 5,000 per hour is the standard value pre-configured for all accounts. Instana recommends that automation and integrations are engineered to respect this quota, using exponential backoff and batching if needed. Values such as 10,000, 6,000, or 1,000 are not defaults, and modifying them requires special support intervention.

NEW QUESTION # 40
In which host agent mode does Instana only monitor the underpinning host and activates its sensors for technologies?

- A. APM
- B. ARM
- C. AWS
- D. INFRASTRUCTURE

Answer: D

Explanation:
The IBM Instana Observability documentation clearly defines several operating modes for the host agent, with INFRASTRUCTURE mode dedicated exclusively to monitoring system-level performance data. The verified extract states: "INFRASTRUCTURE mode configures the host agent to monitor the underlying host metrics and activate sensors for the

technologies running on that host without tracing application-level transactions." It collects CPU, memory, disk, network metrics, and technology integrations like Docker or OS sensors while ignoring application instrumentation. This mode reduces overhead in environments that demand system observability without full APM tracing. APM mode, conversely, extends to application traces and requests. Cloud-specific modes such as AWS or ARM designate external monitoring integrations rather than agent behavior. INFRASTRUCTURE mode thus provides base telemetry visibility as per documented design and was verified in both formulations of the Instana agent guides (v1.0.277, v1.0.307).

NEW QUESTION # 41

.....