Frenquent IBM C1000-189 Update & Practice Test C1000-189 Pdf

DOWNLOAD the newest TestKingFree C1000-189 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1GEwRHalHNdB0wvMVRHdwlDQ809RfDKdA

Our C1000-189 exam torrent is available in PDF, software, and online three modes, which allowing you to switch learning materials on paper, on your phone or on your computer, and to study anywhere and anytime with the according version of C1000-189 practice test. Before you purchase the system, C1000-189 Practice Test provides you with a free trial service, so that customers can fully understand our system before buying; after the online payment is successful, you can receive mail from customer service in 5 to 10 minutes, and then immediately begin to learn C1000-189 training prep.

IBM C1000-189 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Operations: This section of the exam measures the skills of Application Monitoring Specialists and covers daily operational tasks for managing Instana environments. It includes configuring website and application monitoring, handling synthetic monitoring, and creating incidents, issues, and alerts. Candidates will analyze infrastructure performance, set maintenance windows, and design custom dashboards. They are also expected to interpret golden signals, evaluate alerts, use analytics, and perform backup or restore operations to maintain optimal system performance.
Topic 3	• 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 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.
Topic 6	• 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.

Avail Useful Frenquent C1000-189 Update to Pass C1000-189 on the First Attempt

Free update for 365 days is available for C1000-189 study guide, so that you can have a better understanding of what you are going to buy. Through free demo, you can also know what the complete version is like. In addition, with experienced experts to compile the C1000-189 Exam Dumps, quality can be guaranteed. Therefore, if you choose us, you can use them at ease. We have online and offline chat service stuff, who are quite familiar with C1000-189 study guide, if you have any questions, you can consult us.

IBM Instana Observability v1.0.277 Administrator - Professional Sample Questions (Q39-Q44):

NEW QUESTION # 39
What is mandatory to use Instana REST APIs?

- A. CURL
- B. Cookie
- C. Python
- D. Token

Answer: D

Explanation:
Access to Instana's REST API is secured using authorization tokens-an industry-standard best practice for API authentication and traceability. IBM documentation says: "A personal or team API token is required to authenticate REST API calls." Tokens serve as credentials embedded in HTTP headers on each request, providing both identity and access control for the API consumer. Tokens are mandatory; without a valid token, any API requests are denied with a 401 Unauthorized error, regardless of whether a tool (such as CURL) is used. Tokens can be scoped for individual users (personal tokens) or teams (team tokens), enabling granular tracking and revocation as part of enterprise security policies. API tokens are generated from the Instana UI under the profile or team section. Cookies and raw client libraries (e.g., Python) are not authentication methods for Instana APIs.

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

- A. AWS
- B. ARM

- C. INFRASTRUCTURE
- D. APM

Answer: C

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

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

Answer: D

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 # 42
What is the purpose of the configuration option remote_write in Instana when integrated with Prometheus?

- A. To display metrics as only a Prometheus Entity
- B. To configure remote access to Instana
- C. To write data to Prometheus
- D. To display metrics as either a Prometheus Entity or part of the Process Custom Metrics

Answer: D

Explanation:
IBM Instana integrates natively with Prometheus to unify metric ingestion without disrupting existing telemetry setups. The configuration parameter remote_write enables this linkage. The official documentation states: "The remote_write configuration enables Prometheus to send data to Instana, where those metrics are displayed either as Prometheus entities or merged into process custom metrics." Instead of storing them only within Prometheus, Instana pulls remote_write relay feeds to create comprehensive, unified metrics views in its dashboard. This approach avoids duplicate monitoring systems and allows alerting across both Prometheus and Instana data seamlessly. The parameter does not configure outbound writing by Instana back into Prometheus-data always flows from Prometheus to Instana in this architecture. This integration respects Prometheus scraping principles yet centralizes analysis within Instana, achieving correlation between imported numerical time-series values and native metrics at the application or process layer.

NEW QUESTION # 43

What is the purpose of creating a custom service rule in Instana?

- A. To create a manual service configuration
- B. To map services using existing meta-information of the infrastructure component
- C. To apply the service.name tag of the infrastructure component
- D. To set a global service name for all calls

Answer: B

Explanation:

IBM Instana Observability enables users to create custom service rules to precisely associate telemetry with logical services using meta-information already present in infrastructure components. The documentation specifies: "Custom service rules enable mapping of discovered entities to meaningful service constructs, using labels, tags, or annotations present on infrastructure components." This supports the grouping and visualization of traffic/metrics for actual business workflows rather than default technical boundaries. By analyzing meta-data, such as Kubernetes labels, docker tags, or VM metadata, Instana automatically maps relevant requests and traces to the defined service names, improving observability and simplifying troubleshooting. Global service naming (A) and manual configuration (C) do not leverage infrastructure metadata and are not scalable in dynamic environments. Option D relies only on a service.name tag, missing broader meta-information mapping capabilities. The verified documentation supports answer B as the sole comprehensive approach for dynamic service discovery within Instana.

NEW QUESTION # 44

......

id=1GEwRHalHNdB0wvMVRHdwlDQ809RfDKdA