

弊社のIBM C1000-189問題集は通過率が高いです



2026年MogiExamの最新C1000-189 PDFダンプおよびC1000-189試験エンジンの無料共有: https://drive.google.com/open?id=1kDnzbBK4YgvIE_pL4rObx4qEEIfWzgc

IBM Instana Observability v1.0.277 Administrator - Professional衝動的にまたは考慮せずに何かを購入すると、望ましくない選択につながる可能性があります。その結果を防ぐために、IBM Instana Observability v1.0.277 Administrator - Professionalトレーニング資料を用意しました。これらは、保証期間中の専門的な練習資料です。参考のために許容できる価格に加えて、3つのバージョンのすべての資料は、10年以上にわたってこの分野の専門家によって編集されています。さらに、一連の利点があります。したがって、IBM Instana Observability v1.0.277 Administrator - Professionalの実際のテストの重要性は言うまでもありません。今すぐご注文いただいた場合、1年間無料の更新をお送りします。これらのサプリメントはすべて、IBM Instana Observability v1.0.277 Administrator - ProfessionalのC1000-189模擬試験にも役立ちます。

IBM試験に合格し、関連する認定を取得するすべての顧客のニーズを満たすために、当社の専門家はすべての顧客向けに更新システムを設計しました。C1000-189試験問題は毎日更新されます。当社のIT専門家は、C1000-189試験準備が更新されているかどうかを確認する責任を負います。C1000-189テストの質問が更新されると、すぐにシステムがお客様にメッセージを送信します。C1000-189試験準備を使用する場合、更新システムをお楽しみいただき、C1000-189試験にIBM Instana Observability v1.0.277 Administrator - Professional合格することができます。

>> C1000-189模擬対策問題 <<

C1000-189認定テキスト & C1000-189試験勉強攻略

最も少ない時間とお金でIBM C1000-189認定試験に高いポイントを取得したいですか。短時間で一度に本当の認定試験に高いポイントを取得したいなら、我々MogiExamのIBM C1000-189日本語対策問題集は絶対にあなたへの最善なオプションです。このいいチャンスを把握して、MogiExamのC1000-189試験問題集の無料デモをダウンロードして勉強しましょう。

IBM C1000-189 認定試験の出題範囲:

トピック	出題範囲
トピック 1	<ul style="list-style-type: none"> • 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.

トピック 2	<ul style="list-style-type: none"> • 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.
トピック 3	<ul style="list-style-type: none"> • 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.
トピック 4	<ul style="list-style-type: none"> • 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.

IBM Instana Observability v1.0.277 Administrator - Professional 認定 C1000-189 試験問題 (Q54-Q59):

質問 # 54

What is an agile set of focused security and privacy practices that are used by Instana?

- A. Security Orchestration, Automation, and Response
- **B. Security and Privacy by Design**
- C. DevSecOps
- D. Agile Security Practice

正解: B

解説:

IBM Instana observability platform is designed with a strong emphasis on security and privacy best practices. According to the official IBM documentation, Instana applies "Security and Privacy by Design" principles throughout its software lifecycle. The documentation specifically states: "Instana implements security and privacy by design to ensure secure software development, deployment, and system operation, integrating data protection into platform architecture and operations from the outset." This framework mandates data minimization, encrypted in-transit and at-rest telemetry, access control, audit logging, and compliance mapping (such as GDPR or industry frameworks) as default features in Instana platform. While DevSecOps and Security Orchestration are supported concepts, the verified and explicit phrase in IBM Instana documents is Security and Privacy by Design, which is referenced in platform release notes and compliance statements. Agile and focused privacy practices are foundational, as Instana delivers enterprise-grade monitoring for regulated environments.

質問 # 55

What happens if the same key is used in both global and alert-specific custom payload configurations in Instana?

- A. The alert is canceled due to conflict.
- **B. The alert-specific value overrides the global value.**
- C. Both values are concatenated.
- D. The global value overrides the alert-specific value.

正解: B

解説:

IBM Instana documents the merge logic of custom payloads for alerts and global configurations very clearly. The rule states: "If the same key is defined in both a global custom payload and an alert-specific payload, the value from the alert-specific payload will override the global value for that key." This ensures alert context management is precise, enabling targeted incident response with the

most relevant and high-priority data. There is no concatenation, and no alert cancellation or error is triggered as Instana resolves key collisions silently by giving precedence to the more granular, context-specific setting (alert-level). This verified behavior guarantees custom alert events always contain relevant payloads, supporting accurate automated remediation or escalation.

質問 # 56

What is mandatory to use Instana REST APIs?

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

正解: B

解説:

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.

質問 # 57

Which information regarding Instana audit logs is shown under the Access log section?

- A. Adding a new user
- B. New event triggers
- **C. User Login/Logout**
- D. API token creation

正解: C

解説:

Audit logging is a core component of security compliance within IBM Instana. The Access Logs, a section under Audit Logs, are specifically designed to capture and display authentication-related events. IBM states: "Access logs in Instana record user login and logout activity, including timestamps, user IDs, and source IP addresses." This capability supports auditing, regulatory needs, and incident response by ensuring verifiable tracking of system access. Instana separates audit events into categories for clarity: user actions, configuration edits, and security operations, with host-based access details residing in the 'Access Logs' view. This delineation enables administrators to spot unauthorized or suspicious access attempts quickly. Additions of new users or API tokens fall under distinct event categories ('User Management' and 'API Audit Logs') but not under the Access logs specifically. Through its clear segregation of logs by purpose, Instana ensures that organizations maintain compliance with frameworks like ISO 27001, SOC 2, and internal IT governance policy, as access auditability provides both transparency and accountability across multi-user environments.

質問 # 58

Which statement accurately describes the use of the agent key?

- A. It is not included in the purchase email and must be obtained separately.
- B. It is used only for deploying an instance.
- C. It is required only for downloading the license.
- **D. It is used for both downloading Instana artifacts and deploying an instance.**

正解: D

解説:

The IBM Instana Observability product architecture uses a security credential called an agent key for authentication and authorization in both installation and deployment operations. The documentation explicitly affirms: "The agent key must be used for

