

DUMPS ARENA

IBM Instana Observability v1.0.277 Administrator – Professional

IBM C1000-189

Version Demo

Total Demo Questions: 7

Total Premium Questions: 78

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture	19
Topic 2, Installation	9
Topic 3, Configuration	33
Topic 4, Administration	16
Topic 5, Troubleshooting	1
Total	78

QUESTION NO: 1

An organization monitors workloads in several AWS Regions, including event-driven functions. The administrator wants to use supported Instana monitoring approaches while controlling CloudWatch collection independently where required. Which two statements are correct? Select two.

- A. AWS Lambda can be monitored by using Instana serverless agents.
- B. CloudWatch API polling intervals can be configured at the Region level.
- C. A host agent must run inside each Lambda function to monitor invocations.
- D. CloudWatch API polling intervals can be configured only at the resource-group level.
- E. AWS Lambda monitoring requires an Application Perspective before telemetry is collected.

ANSWER: A B

Explanation:

Instana supports serverless monitoring for **AWS Lambda**. CloudWatch API polling intervals can be configured at the **Region** level, which allows collection cadence to differ between Regions. A Lambda function does not require a continuously running host agent inside the function, and polling configuration is not defined at a resource-group level.

QUESTION NO: 2

What are the two SLI types Instana supports while configuring the service level objectives?

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

ANSWER: C D

Explanation:

Instana supports **Time based** and **Event count based** service level indicators when configuring service level objectives. A time-based SLI measures the proportion of time during the SLO evaluation window in which a specified condition is satisfied. This is appropriate for objectives expressed in terms of sustained availability or health, where the important question is how long a service met its expected state. An event count-based SLI evaluates a population of observed events and determines the proportion that meet the defined success criteria. This model is suited to objectives based on transactions, requests, calls, or other measurable event outcomes, such as the percentage of successful requests or requests completed within a performance threshold. Together, these SLI models let administrators define objectives either from compliance over time or from the quality of individual observed events. IBM's Instana documentation describes SLO configuration and the available SLI approaches in its Service Level Objectives guidance: [IBM Instana Service Level Objectives](#). Additional IBM documentation for Instana observability features is available at [IBM Instana Observability documentation](#).

QUESTION NO: 3

A Prometheus server is configured to send samples to Instana by using remote write. The administrator wants the received metrics to appear with the monitored workload rather than attempting to send data from Instana back to Prometheus. What is the purpose of the Instana `remote_write` configuration?

- A. To write Instana metrics back to the Prometheus server

- B. To select whether received metrics are shown as a Prometheus Entity or Process Custom Metrics
- C. To configure remote administrator access to the Instana backend
- D. To expose only host-level resource metrics to Prometheus

ANSWER: B

Explanation:

The `remote_write` configuration controls how Prometheus remotely written metrics are modeled in Instana: as a Prometheus Entity or as Process Custom Metrics. Prometheus remote write sends samples to a remote receiver; in this integration, Instana receives and displays those samples. It does not configure remote access to Instana or cause Instana to write telemetry back to Prometheus.

QUESTION NO: 4

A Synthetic test that normally runs from an internal Point of Presence stops executing after the PoP is removed during infrastructure maintenance. Which Instana event provides the automatic operational indication of this condition?

- A. Synthetic pop status
- B. Offline event detection system rule
- C. Application Perspective availability event
- D. Custom metric threshold event

ANSWER: A

Explanation:

The built-in **Synthetic pop status** event automatically reflects the operational status of a Synthetic PoP, including when the PoP is uninstalled. Creating a separate Offline detection rule or manually triggering an event is unnecessary for this PoP lifecycle condition.

QUESTION NO: 5

Which language is primarily used for writing Synthetic monitoring API scripts in Instana?

- A. Java
- B. JavaScript
- C. Python
- D. Go

ANSWER: B

Explanation:

JavaScript is primarily used for Instana Synthetic Monitoring API scripts. Instana supports scripted API tests for situations in which a simple HTTP check is insufficient and custom logic is needed to build requests, handle responses, extract values, perform assertions, and control the test flow. The scripting environment is based on JavaScript, enabling a monitor to programmatically execute API interactions and determine whether the monitored service behaves as expected. This makes JavaScript appropriate for sophisticated synthetic scenarios, such as obtaining an authentication token, passing data from one request to a subsequent request, validating a response body, or applying custom success criteria. JavaScript is also the language used for browser-scripted synthetic tests, providing a consistent scripting approach across Instana synthetic monitoring capabilities. Administrators should therefore use JavaScript when creating a Synthetic monitoring API script

rather than selecting a general-purpose application language. IBM's Synthetic Monitoring documentation describes the available API-test types and scripted test configuration, while the Instana documentation landing page provides the versioned product documentation for synthetic monitoring features. See [IBM Instana Synthetic Monitoring documentation](#) and [IBM Instana Observability documentation](#).

QUESTION NO: 6

Which statement is true about webhook URL authentication?

- A. Prepend username and password to the hostname URL for authentication.
- B. Specification of additional Headers is not supported for authentication.
- C. Only Authorization HTTP request header is supported.
- D. Basic authentication is not supported due to security constraints.

ANSWER: A

Explanation:

Prepend username and password to the hostname URL for authentication. This is the documented configuration method for an Instana webhook endpoint that requires HTTP Basic Authentication. The credentials are included in the URL user-information portion, before the hostname, using a form such as `https://username:password@webhook.example/path`. When Instana sends the webhook request, these credentials allow the receiving endpoint to authenticate the request according to the HTTP Basic Authentication scheme. This configuration is particularly useful for webhook receivers that protect an endpoint with a username and password but do not require a separate token-exchange flow. The URL must still be a valid endpoint URL, and the username and password must be correctly encoded when they contain characters with special meaning in URLs. As with any credential-bearing configuration, administrators should use a secured HTTPS endpoint and protect access to the Instana configuration because the URL contains authentication-sensitive information. IBM's webhook integration documentation describes placing the username and password before the webhook hostname for this purpose. See the IBM documentation for [Webhook integration](#) and the HTTP standard's definition of URI user information in [RFC 3986, section 3.2.1](#).

QUESTION NO: 7

A team installs a Synthetic PoP by using Helm and wants its deployment configuration to be repeatable while still allowing a small emergency override during installation. Which two Helm mechanisms can be used to supply chart values? Select two.

- A. Provide a YAML values file with the `-f` flag.
- B. Specify an individual value with the `--set` flag.
- C. Provide a configuration file with the `--config` flag.
- D. Modify the chart defaults directly before every installation.
- E. Pass all chart values only through environment variables.

ANSWER: A B

Explanation:

The `-f` flag supplies a YAML values file, which is appropriate for reviewed and reusable configuration. The `--set` flag supplies a command-line value override for targeted changes. Helm does not require direct modification of the chart package, and `--config` is not the standard Helm mechanism for supplying chart values.