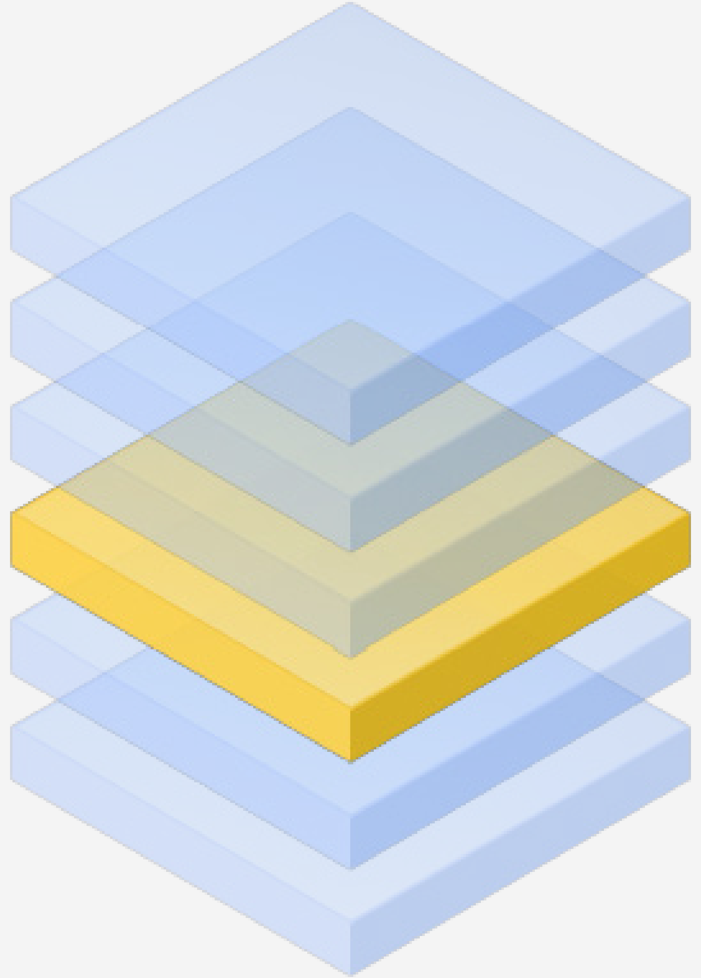
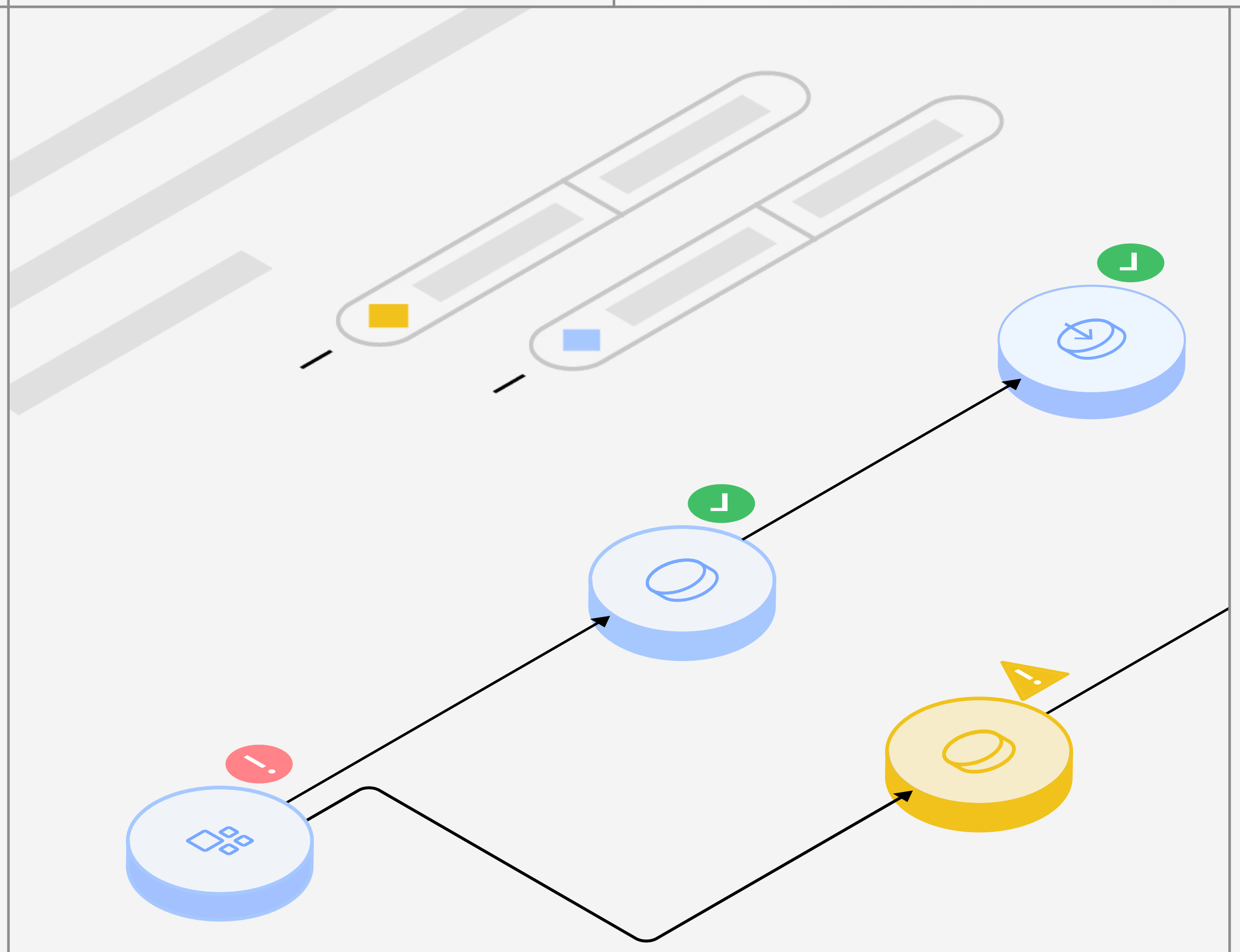
A DevOps guide to full-stack observability



Fix what you can't see with AI



IBM

Contents

01

Full-stack observability

So much to see, so much to do—
so little time

Full-stack application observability gives you the ability to monitor, analyze and understand the performance and behavior of an entire application stack—from the interface to the underlying infrastructure.

But, as a DevOps professional, you face three primary challenges when it comes to full-stack application observability.

1. **Complexity of modern applications**
   Modern applications are increasingly complex, which makes it difficult to monitor and analyze the entire stack, leading to blind spots that hinder your ability to identify and resolve issues quickly and easily.

2. **Data volume and noise**
   Full-stack observability generates a vast amount of data from various sources, including metrics, logs and traces. Sifting through this data and noise to identify relevant information can be overwhelming.

3. **Lack of context and correlation**
   Data from different sources lacks context so it can be difficult to interpret and identify the root cause of problems, which can lengthen mean-time-to-resolve (MTTR) issues.

How do you alleviate these challenges?
With AI. AI-driven application observability can help you detect and investigate failures in your applications, cloud environment, infrastructure and digital experiences early to accelerate root cause analysis and remediation. AI can also help optimize alerting practices to reduce the noise so you can identify and resolve issues in real time to reduce downtime and outages—and improve the overall user experience.

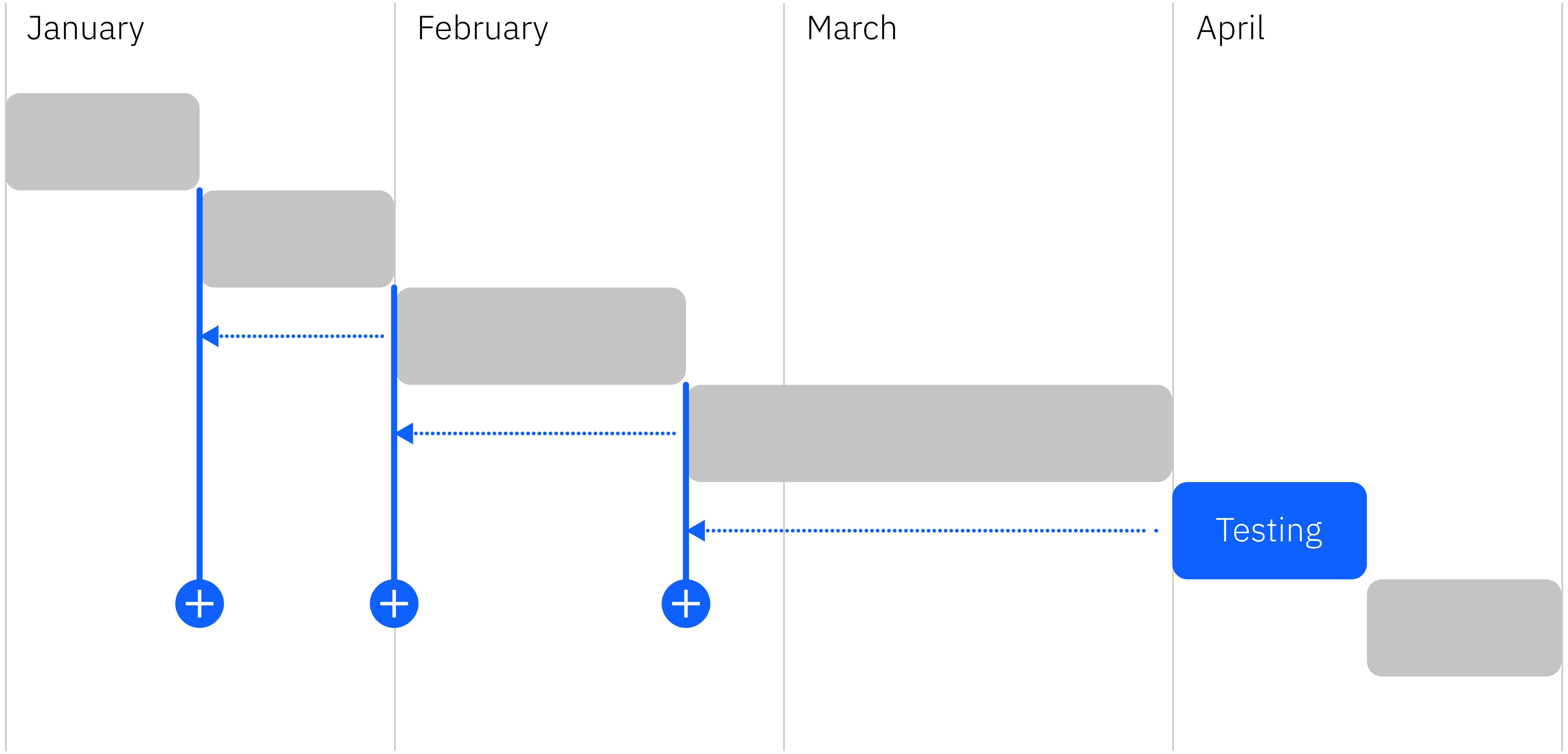
02

Shift-left observability

Are you ready to stop playing catch-up?

Picture a development culture where you can make adjustments and improvements early and continuously.

Shift left in the context of agentic AI and application observability refers to the practice of integrating testing, security and observability early in the development lifecycle.



By adopting a shift-left approach, you can build more robust, reliable and observable agentic AI applications that meet business needs and user expectations.

1 Detecting potential issues early and proactively addressing them before they become significant problems

2 Helping ensure that quality is built into the application, environment or experience from the outset to reduce the likelihood of downstream issues

3 Promoting collaboration between stakeholders to help ensure that everyone is aligned and working toward the same goal

03

Incident investigation in action

Solve problems under pressure

Does this scenario sound familiar?

It’s morning on Black Friday, and your e-commerce platform traffic is surging. Sales are spiking. Then—without warning—key pages start timing out.

Your site reliability engineer is combing through logs. Your manager gets pulled into an emergency meeting. Your CIO is panicking. But what if you didn’t have to start from scratch to figure out the problem?

Instead of jumping between dashboards or manually tracing anomalies, an autonomous AI agent analyzes dependencies, detects patterns and pinpoints the root cause in real time. You’re not chasing problems—you’re guiding the AI as it investigates, understands and resolves the incident.

Crisis averted. Revenue protected. And what normally would’ve taken hours to resolve is addressed in minutes.

04

Best practices for full-stack observability

Make the most out of your full-stack observability journey

This list outlines best practices for maximizing observability to discover root causes, reduce alert fatigue, strengthen system resilience and deliver a better user experience, so you can move from reactive firefighting to proactive optimization.

1

Comprehensive instrumentation
Ensure you have comprehensive monitoring of your entire application stack—including all services, APIs, databases and infrastructure components.

2

Leverage health indicators
Use health indicators to set up alerts to proactively identify and resolve issues.

3

Understand trace context
Understand how to read and interpret traces in context to follow requests through your system for better troubleshooting.

4

Regularly review dashboards and reports
Gain insights into your application's performance and behavior over time by identifying trends, anomalies and potential problems early.

5

Take advantage of integration capabilities
Use the provided integrations to enrich your data and gain a more holistic view of your system.

6

Optimize alerts
Tailor real-time alerts and dashboards to focus on what matters most for your specific application and business needs to avoid alert fatigue.

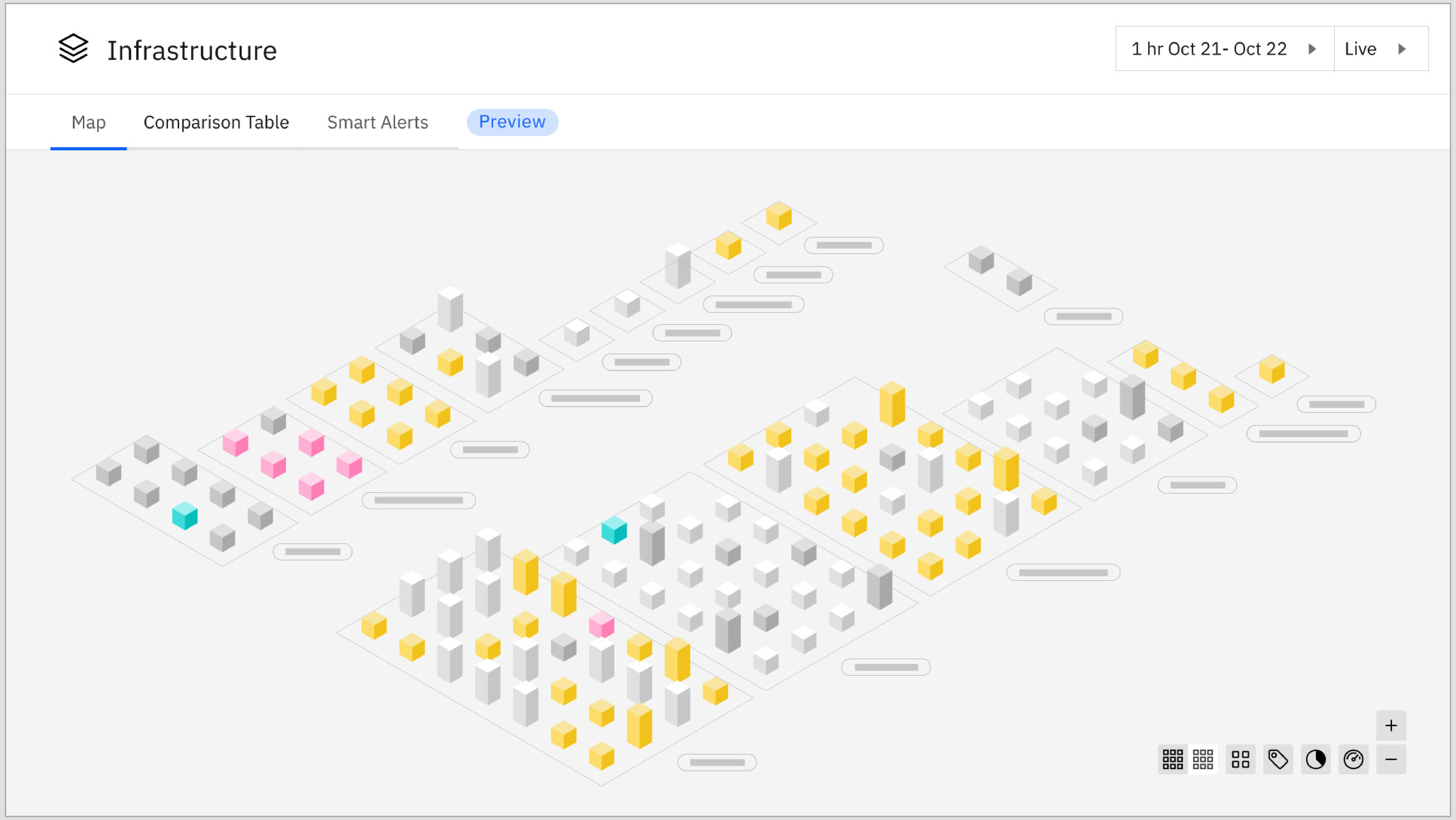
05

IBM Instana

Meet IBM Instana. Your dynamic partner in the fast-paced development landscape. AKA, your new best friend.

IBM Instana® Observability is an automated observability solution that provides advanced application performance monitoring and observability capabilities.

It gives DevOps teams real-time visibility into application and infrastructure performance to help them identify and resolve issues quickly.



With an intuitive interface and automated insights, Instana makes it easier for DevOps professionals to understand complex system behaviors.

Automated application performance management for microservices and cloud-native applications

Incident discovery using a single agent for each host

The ability to monitor applications, infrastructure, services and systems

Real-time collection and correlation of metrics, events, logs and traces (MELT) data using auto-instrumentation and auto-discovery

Alerting and notification capabilities with thresholds based on risk and impact

Source-code-level visibility into over 300 third-party technologies and IBM proprietary software and infrastructure

300+ technologies supported by IBM Instana

Learn more →

.NET Core, .NET Full Framework, ActiveMQ, ActiveMQ Artemis, Aerospike, IBM AIX®, Akka, Akka HTTP, Alibaba Cloud Object Storage Service (OSS), Amazon Corretto, Amazon EKS Anywhere, Amazon ElastiCache, Amazon OpenSearch, Amazon SNS, Red Hat® Ansible, Apache CXF, Apache HBase, Apache Kafka, Apache Spark, Apache Tomcat, Apache Web Server, APM (Coralogix), APM (Humio), APM (Splunk), APM (LogDNA), Aqua Security, Axis2, Amazon Web Services (AWS), AWS Beanstalk, AWS EC2, AWS ELB, AWS Fargate, AWS Kinesis, AWS Lambda, AWS MQ, AWS RDS, AWS S3, AWS SQS, Azure AKS, Azure CosmosDB, Azure Functions, Azure Queue Storage, Azure SQL Database, Azure SQL Elastic Database Pool, BEA JRockit, Camel, Cassandra, Red Hat® Ceph®, Chef, ClickHouse, Cloud Foundry, Clojure, CockroachDB, Consul, Containerd, CoreOS, CoreOS Tectonic, CORBA (Sun), Couchbase, CRI-O, DC/OS, Docker, Dropwizard, DynamoDB, Eclipse OpenJ9, Ehcache, etcd, FaunaDB, Feign, Giant Swarm, GlassFish, GO, Google Cloud Datastore, Google Cloud Platform (GCP), Google Cloud Storage, Google Compute Engine (GCE), Google Kubernetes Engine (GKE), GraphQL, HAProxy, Hangfire, Hadoop YARN, Hashicorp, HornetQ, IBM Cloud®, IBM Concert®, IBM Db2®, IBM Cloud Kubernetes Service, IBM Instana® Logs in Context, IBM J9, IBM Kubecost, IBM Turbonomic®, IBM MQ, IBM webMethods, IBM z/OS® IIS (Microsoft), Instana AutoProfile, Instana AutoTrace, Jaeger, Java, Jersey, Jetty, Red Hat® JBoss®, JBoss Data Grid, JBoss WildFly, JVM, Kubernetes, Linux®, Liferay, LogDNA, MariaDB, Marathon, Memcached, Microsoft .NET, Microsoft Message Queue, Microsoft Office 365, Microsoft SQL Server, Microsoft Teams, Microsoft Windows Server, MongoDB, MuleSoft, MySQL, NATS, Neo4j, Node.js, Nomad, OpenCensus, OpenLDAP, OpenSearch, OpenTelemetry, OpenTracing, Oracle Cloud, Oracle Database, Oracle OKE, OSProcess, PagerDuty, PCF (VMware Tanzu), PHP, PostgreSQL, Prometheus, Puppet, Python, Rancher, RatPack, ReactiveMongo, Red Hat®, Redis, Redis Enterprise, Redis Lettuce, Ruby, SAP HANA, Scala, ServiceNow, Slack, Solaris, Solr, SQL Anywhere, StatsD, Sun ONE Server, Sybase SQL Anywhere, TIBCO EMS, TIBCO ESB, Tomcat, Traefik Labs, Unix System, Vaadin, Varnish, VictorOps, VMware Tanzu, VMware Tanzu PKS, Webex Teams, Webhooks, WebMethods Glue, Wicket, Zipkin, Zookeeper

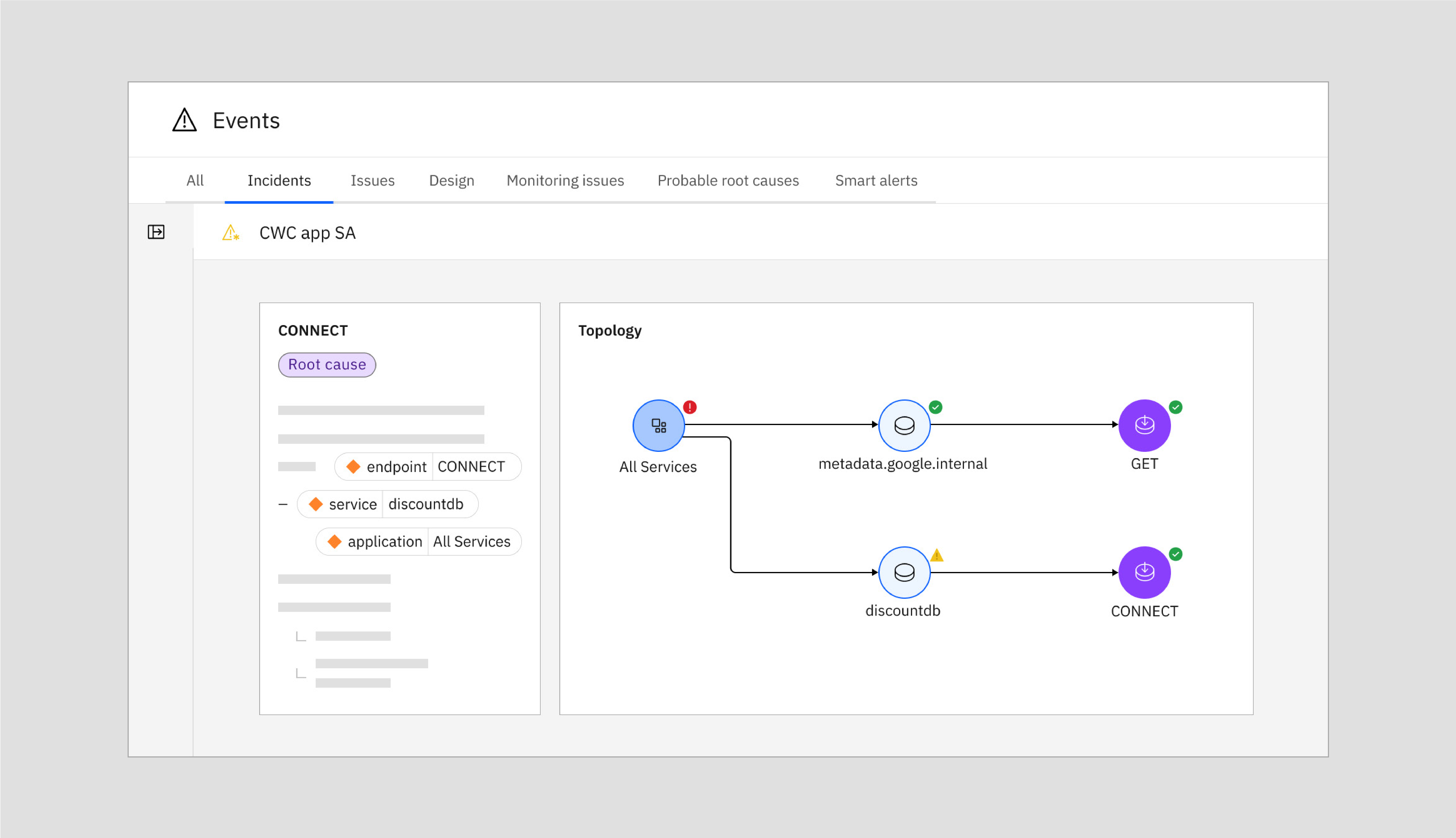
06

Intelligent incident investigation powered by agentic AI

Know what broke where and why—before it impacts users—with IBM Instana

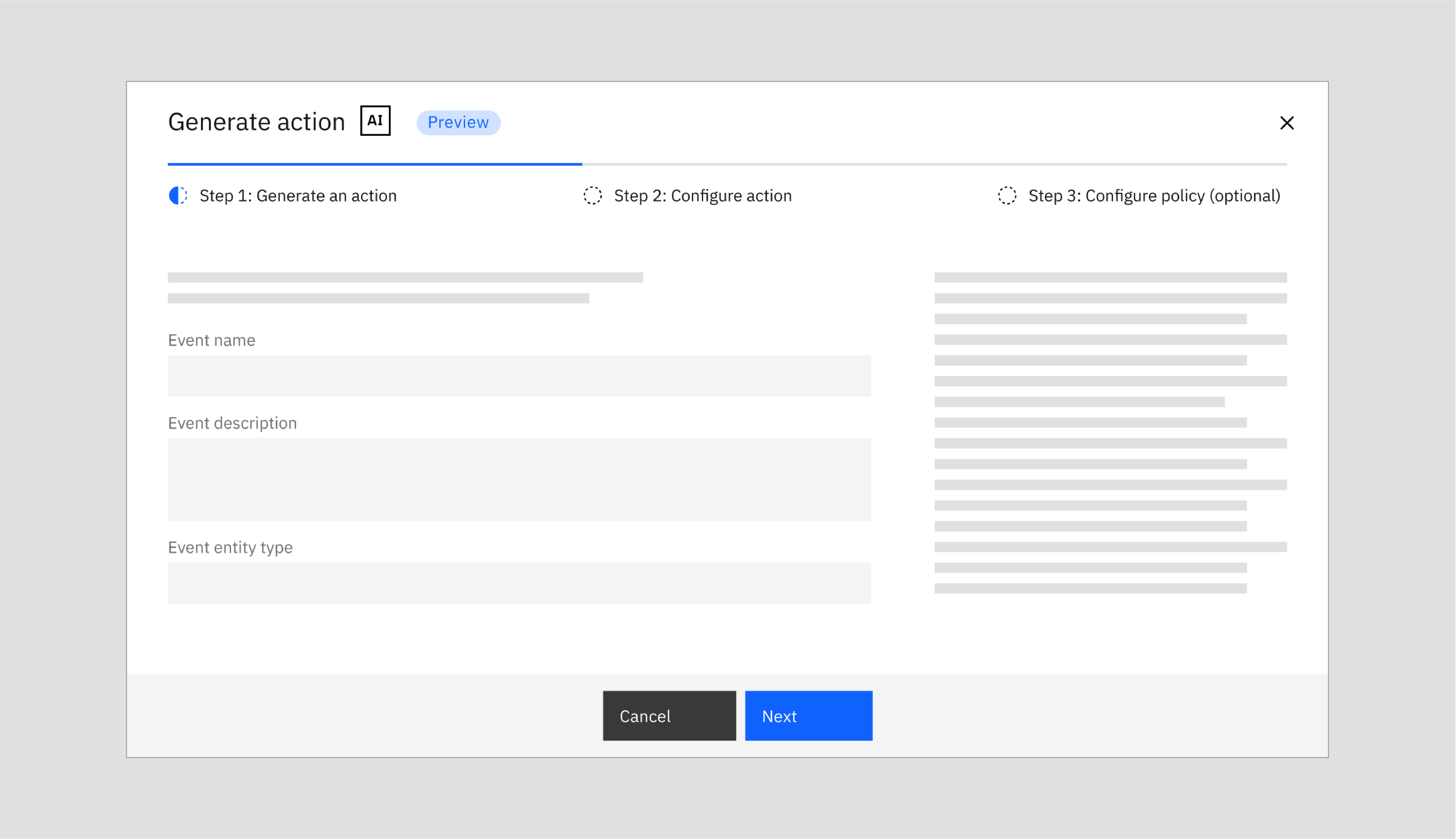
You can launch an automated investigation into any incident using the IBM Instana Intelligent Incident Investigation solution, powered by agentic AI.

From there, Instana builds a hypothesis to identify details of the problem, its location and impact, as well as the AI agent's reasoning and actions to deliver comprehensive, contextual information about the incident in seconds.



1

Remediate problems faster using a step-by-step runbook of actions.



Generate action AI Preview

Step 1: Generate an action
Step 2: Configure action
Step 3: Configure policy (optional)

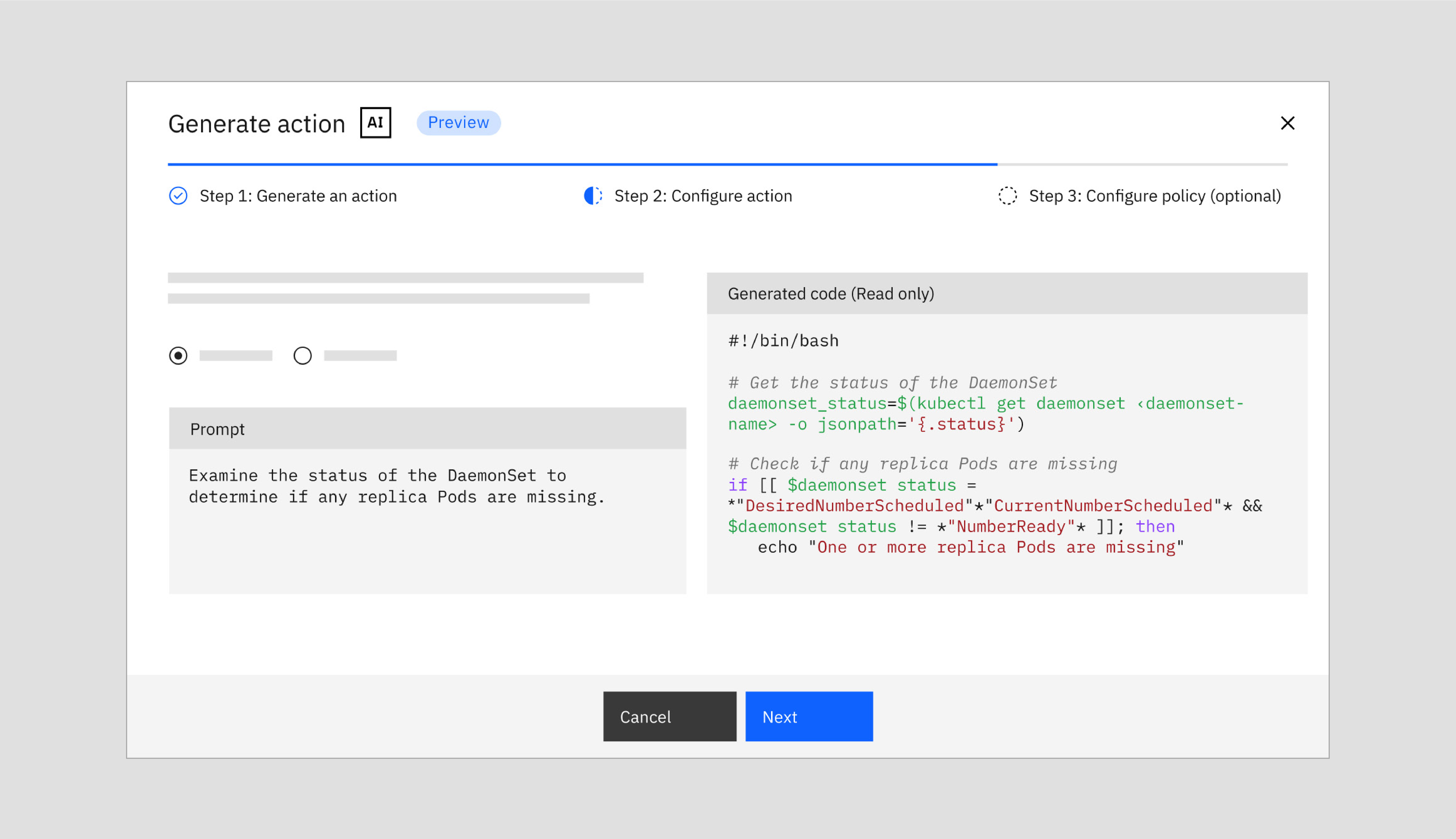
Event name:

Event description:

Event entity type:

2

Create a Bash script for each step and export it to GitHub for review, testing and deployment.


Generate action AI Preview
×
Step 1: Generate an action
Step 2: Configure action
Step 3: Configure policy (optional)
● ○

Prompt

Examine the status of the DaemonSet to determine if any replica Pods are missing.

Generated code (Read only)

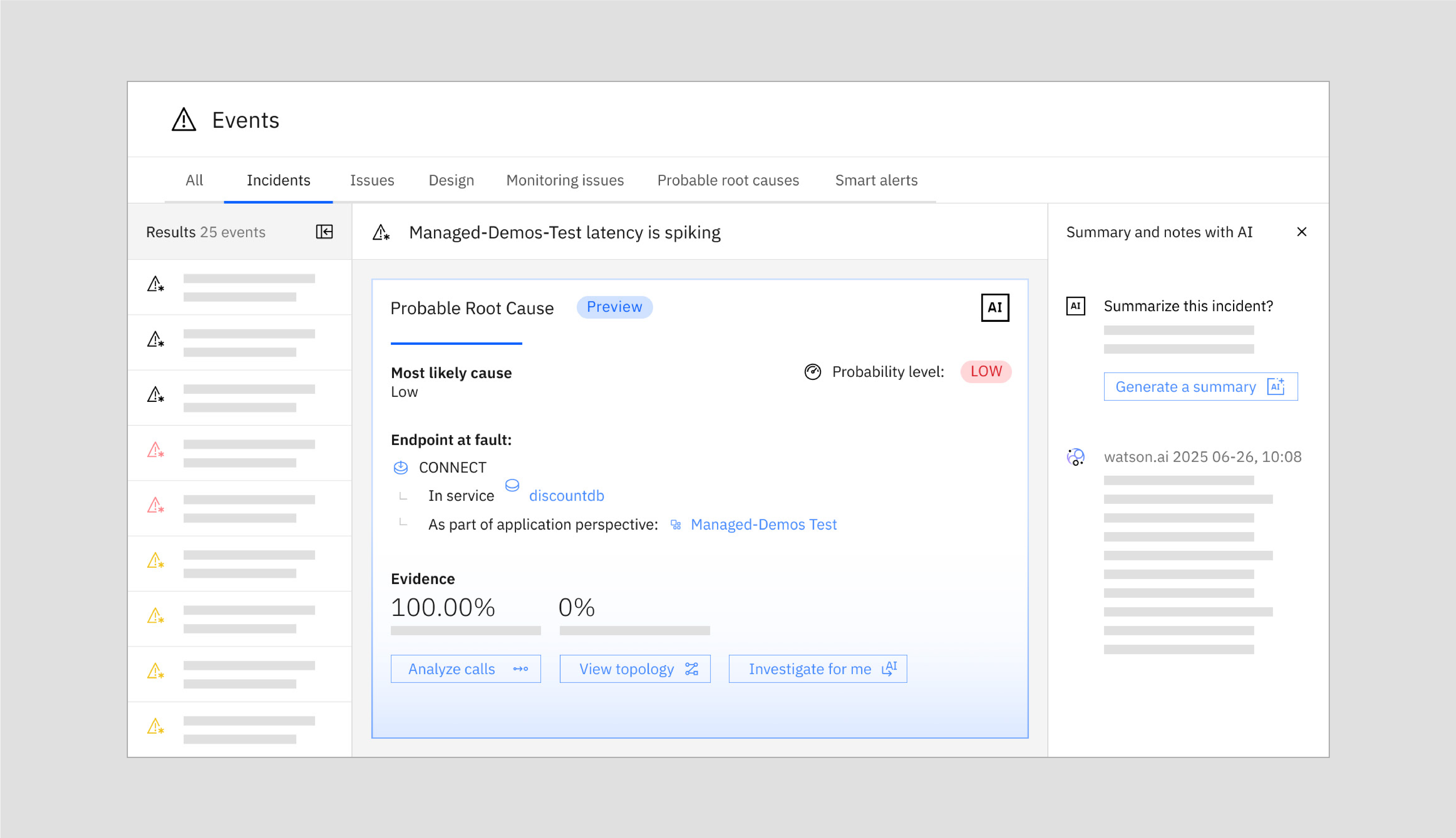
```
#!/bin/bash

# Get the status of the DaemonSet
daemonset_status=$(kubectl get daemonset ‹daemonset-
name> -o jsonpath='{.status}')

# Check if any replica Pods are missing
if [[ $daemonset status =
*"DesiredNumberScheduled"*"CurrentNumberScheduled"* &&
$daemonset status != *"NumberReady"* ]]; then
   echo "One or more replica Pods are missing"
```

3

Let the report write itself with an incident summary that includes key information.



Managed-Demos-Test latency is spiking

Probable Root Cause

Most likely cause
Low

Probability level: LOW

Endpoint at fault:

CONNECT

In service discountdb

As part of application perspective: Managed-Demos Test

Evidence

100.00% 0%

Summarize this incident?

watson.ai 2025 06-26, 10:08

07

Conclusion

Conclusion

Let’s face it—modern IT environments are complicated. That’s why weaving smart, AI-driven observability into your entire stack isn’t just helpful, it’s essential. When you shift left and build quality into your pipeline from the start, you’re more equipped to catch issues early, fix them quickly and keep everything running smoothly.

IBM Instana can enable these strategies and give you comprehensive, real-time visibility across the complete application development lifecycle so you can detect anomalies more easily, resolve issues faster and continuously optimize performance.

Why wait? Step into the future of DevOps where technology works with you to deliver better performance, greater reliability and a future-ready foundation. Ready to find more, fix more and do more with Instana? Don’t just take our word for it. See it for yourself.

Try the IBM Instana sandbox →

Learn more about IBM Instana →

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.