DUMPSBOSS.

VMware Tanzu for Kubernetes Operations Professional

VMware 2V0-71.23

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, IT Architectures, Technologies, Standards	4
Topic 2, VMware by Broadcom Solution	2
Topic 3, Install, Configure, and Setup	7
Topic 4, Performance-tuning, Optimization, and Upgrades	3
Topic 5, Troubleshooting and Repairing	4
Topic 6, Administrative and Operational Tasks	3
Total	23

QUESTION NO: 1

A team uses Harbor as the registry for images deployed to Tanzu Kubernetes clusters. Which two controls reduce the risk of deploying images with known vulnerabilities or images that have been replaced under an existing tag? (Choose two.)

A. Enable vulnerability scanning for registry projects.

B. Allow insecure registry connections from every cluster.

C. Configure tag immutability rules for released images.

D. Grant anonymous users permission to push images.

E. Disable image content verification for deployment pipelines.

ANSWER: A C

Explanation:

Harbor vulnerability scanning identifies known vulnerabilities in stored images and provides information that can be used in image admission and deployment decisions. Tag immutability prevents a user from replacing an image that already has a protected tag, which helps ensure that a referenced image tag remains stable.

Using insecure registry access weakens transport security. Granting anonymous push access removes accountability and control over image publication. Disabling content trust does not protect image integrity.

QUESTION NO: 2

What statement describes the role of VMware Aria Operations for Applications (formerly VMware Tanzu Observability) in VMware Tanzu for Kubernetes Operations?

A. Watches defined infrastructure systems to keep track of health of resources.

B. Automates the remediation of Kubernetes platform resources based on collected data.

C. Tracks metrics, logs, and alerts based on specified thresholds.

D. Collects and analyzes traces, metrics, and logs to provide single source of truth for actionable insights.

ANSWER: D

Explanation:

Collects and analyzes traces, metrics, and logs to provide single source of truth for actionable insights. This accurately describes VMware Aria Operations for Applications, previously called Tanzu Observability by Wavefront. It is a SaaS-based observability platform that ingests high-volume telemetry from Kubernetes environments, applications, infrastructure, and cloud services. By correlating metrics with distributed traces and logs, it helps platform and application teams investigate the behavior, performance, and availability of workloads across the full application stack.

Its value in Tanzu for Kubernetes Operations is the unified operational visibility it provides: teams can explore telemetry, build custom dashboards, define alert conditions, and troubleshoot incidents using contextual data rather than relying on disconnected monitoring tools. Distributed tracing is particularly important for modern microservices because it follows requests across service boundaries and helps identify where latency or errors occur. The platform therefore delivers actionable insights from observability data for both Kubernetes platform operations and application operations. VMware documentation describes Tanzu Observability as a platform for monitoring and analyzing metrics, histograms, traces, and spans: VMware Tanzu Observability documentation. Additional Tanzu Kubernetes Operations observability guidance is available from Broadcom Tanzu Kubernetes Operations documentation.