2V0-71.23Q&As

VMware Tanzu for Kubernetes Operations Professional

Pass VMware 2V0-71.23 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/2v0-71-23.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What two steps are required to visualize API connectivity and enable API protection in VMware Tanzu Service Mesh? (Choose two.)

A. Activate API Discovery for the Global Namespace

B. Create API Security Policy for the Global Namespace

C. Enable Threat Detection Policy for the Global Namespace

D. Set a Distributed Firewall policy for the Global Namespace

E. Create an Autoscaling policy for API for the Global Namespace

Correct Answer: AB

To visualize API connectivity and enable API protection in VMware Tanzu Service Mesh, the administrator needs to perform two steps: Activate API Discovery for the Global Namespace. This allows Tanzu Service Mesh to automatically discover the APIs signatures between microservices running inside or outside the mesh. API Discovery creates a custom API schema for each API that is close to OpenAPI spec 3.0. Tanzu Service Mesh graph renders the detected APIs in the Enforcing mode by default, which means that any new API is considered as a violated API unless accepted by the administrator1 Create API Security Policy for the Global Namespace. This allows the administrator to block or allow layer 4 and layer 7 traffic, as well as create granular policies that provide API and data segmentation, OWASP 10 attack defense, schema validation, geofencing, data compliance, and egress controls. The administrator can create the API Security policy through the Tanzu Service Mesh Console UI or by using the Tanzu Service Mesh API Explorer2 References: 1: https:// docs.vmware.com/en/VMware-Tanzu-Service-Mesh/services/tanzu- service-mesh-enterprise/GUID-E6FB9FB3-FDB3-4D2B-B5CB-614608EEF537.html 2: https://docs.vmware.com/en/VMware-Tanzu-Service-Mesh/services/tanzu-service-mesh- enterprise/GUID-5B635420-3BD2-4EC1-B67E-2015F991A91C.html

QUESTION 2

A Tanzu Mission Control administrator would like to enforce the following container controls:

1.

Only allows container images that match the specified names or tags.

2.

Ensure that the container image is not tampered with.

Which type of policy can be used?

A. Access

B. Security

C. Image Security

D. Image Registry

E. Network

Correct Answer: C

The type of policy that can be used to enforce the container controls is image security. Image security policies allow users to define rules for validating container images before they are deployed on clusters. Users can specify image names, tags, signatures, or digests to whitelist or blacklist images based on their source and integrity. Users can also enable or disable image scanning for vulnerabilities and configure the severity threshold for admission decisions. References: Image Security Policy - VMware Docs, Image Policy - VMware Docs

QUESTION 3

Which statement is true about Tanzu package CLI plugin?

A. It cannotbe used to add additional package repositories apart from tanzu-standard.

B. It can be used to manage packages in public repositories.

C. It is intended only for CLI-managed packages.

D. It can be used to install auto-managed packages.

Correct Answer: C

The Tanzu package CLI plugin is a tool that allows users to install and manage Tanzu packages on their clusters. Tanzu packages are Kubernetes resources that encapsulate the deployment and configuration of software components, such as Contour, Prometheus, Grafana, and more1. The Tanzu package CLI plugin is intended only for CLI- managed packages, which are packages that users can install and update manually using the Tanzu CLI commands2. The Tanzu package CLI plugin cannot be used to install or manage auto-managed packages, which are packages that are automatically installed and updated by Tanzu Kubernetes Grid as part of the cluster lifecycle2. The other options are incorrect because: It cannot be used to add additional package repositories apart from tanzu-standard is false. The Tanzu package CLI plugin can be used to add, list, update, or delete package repositories, which are sources of Tanzu packages3. Users can add custom package repositories or use the default tanzu-standard repository that comes with Tanzu Kubernetes Grid4. It can be used to manage packages in public repositories is false. The Tanzu package CLI plugin can only be used to manage packages in the repositories that are added to the target cluster3. Users cannot use the Tanzu package CLI plugin to manage packages in public repositories that are not added to the cluster. It can be used to install auto-managed packages is false. As mentioned above, the Tanzu package CLI plugin cannot be used to install or manage auto-managed packages. References: Tanzu Packages, Tanzu Package Types, tanzu package repository, Add a Package Repository

QUESTION 4

What is the Kubernetes component that is responsible for workload creation?

A. API Sep/er

B. Scheduler

C. etcd

D. Kubelel

Correct Answer: B

The Scheduler is the Kubernetes component that is responsible for workload creation. The Scheduler is responsible for

assigning pods to nodes based on various factors, such as resource availability, node affinity, taints and tolerations, and pod priority. The Scheduler watches for newly created pods that have no node assigned, and selects a suitable node for them to run on. The Scheduler then informs the API server of its decision, and the API server binds the pod to the node. References: Scheduling | Kubernetes, Kubernetes Components | Kubernetes

QUESTION 5

What is the role of Prometheus in a VMware Tanzu Kubernetes Grid cluster?

A. Provide the functionality of a lightweight log processor and forwarder that allows you to collect data and logs from different sources.

B. Collect metrics from target clusters at specified intervals, evaluate rule expressions, display the results, and trigger alerts if certain conditions arise.

C. Inject time-series database (TSDB) data into high-quality graphs and visualizations.

D. Extend the open-source Docker distribution by adding the functionalities usually required by users such as security and identity control and management.

Correct Answer: B

Prometheus is an open-source systems monitoring and alerting toolkit that can collect metrics from target clusters at specified intervals, evaluate rule expressions, display the results, and trigger alerts if certain conditions arise8. Tanzu

Kubernetes Grid includes signed binaries for Prometheus that users can deploy on workload clusters to monitor cluster health and services9. Prometheus uses a pull model to scrape metrics from various sources, such as Kubernetes nodes,

pods, services, and endpoints. Prometheus stores the collected metrics in a time-series database and allows users to query them using PromQL, a powerful query language. Prometheus also supports defining alert rules based on metric

values and sending notifications to external systems, such as Alertmanager8.

The other options are incorrect because:

Provide the functionality of a lightweight log processor and forwarder that allows you to collect data and logs from different sources is a description of Fluent Bit, which is an open-source log processor and forwarder that can be used to collect

data and logs from Kubernetes clusters and send them to various destinations10. Fluent Bit is not part of Tanzu Kubernetes Grid. Inject time-series database (TSDB) data into high-quality graphs and visualizations is a description of Grafana,

which is an open-source visualization and analytics software that can be used to query, visualize, alert on, and explore metrics from various sources, including Prometheus11. Grafana is not part of Tanzu Kubernetes Grid.

Extend the open-source Docker distribution by adding the functionalities usually required by users such as security and identity control and management is a description of Harbor, which is an open-source cloud native registry that can be

used to store, sign, and scan container images for vulnerabilities12. Harbor is not part of Tanzu Kubernetes Grid.

References: Prometheus Overview, Implement Monitoring with Prometheus and Grafana, Fluent Bit, What is Grafana?, Harbor Overview

[2V0-71.23 PDF Dumps](#) [2V0-71.23 Study Guide](#) [2V0-71.23 Exam Questions](#)