KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **Portworx Enterprise Professional**

Title : Pure Certified Portworx Enterprise Professional (PEP) Exam

Version : DEMO

1.A Portworx administrator wants to control which nodes will host a KVDB installation.
What steps must an administrator take to ensure that KVDB installs on NODE01, NODE03, and NODE05?
A. It is not possible to configure the location of the KVDB prior to installation.
B. Change the following in the 'StorageCluster' spec prior to installation:
spec:
kvdb:
selector:
matchNodeName:
- NODE01
- NODE03
- NODE05
C. Label NODE01, NODE03, and NODE05 with 'px1/metadata-node=true' prior to installation.
Answer: B
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Portworx provides a mechanism to control KVDB pod placement through the kvdb.selector.matchNodeName field in the StorageCluster Custom Resource Definition (CRD). This allows administrators to explicitly specify node names where KVDB pods will be deployed. By setting this selector to include NODE01, NODE03, and NODE05, KVDB pods will run exclusively on these nodes, ensuring better control of quorum, fault tolerance, and performance. Node labeling alone is insufficient unless the labels are properly referenced in the spec, making direct node name matching the most straightforward and reliable method. This configuration must be done prior to cluster installation to ensure proper pod placement. Official Portworx documentation on cluster deployment and KVDB configuration confirms this method as the recommended best practice for managing KVDB nodes, critical for maintaining database availability and consistency within the Portworx cluster【Pure Storage Portworx Install Guide†source】.

2.What is the name of the Kubernetes secret containing external KVDB certificates?
A. px-kvdb
B. px-kvdb-cert
C. px-kvdb-auth
Answer: C
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The Kubernetes secret named px-kvdb-auth is used to store external KVDB certificates in a Portworx deployment. These certificates enable mutual TLS authentication for the KVDB pods, ensuring secure and authenticated communication between the distributed KVDB instances running on different nodes. The px-kvdb-auth secret includes private keys and certificate chains that are essential for encrypting KVDB traffic and verifying peer identities within the cluster. This security feature prevents unauthorized access and protects sensitive KVDB data in transit. Portworx's official security and KVDB documentation detail the use of this secret, highlighting its role in certificate management and enabling encryption for high-availability clusters running on Kubernetes environments【Pure Storage Portworx Security Guide†source】.

3.How should a Portworx administrator expose metrics to externally provisioned Prometheus?
A. Enable metrics in the storagecluster object by setting the following:
spec:
monitoring:
prometheus:
exportMetrics: true
B. Enable metrics in the storagecluster object by setting:
spec:
monitoring:
exportMetrics: true
C. Enable metrics in the Portworx cluster by running the command:
pxctl service monitoring enable --export-metrics-only
Answer: A
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To enable Portworx metrics exposure compatible with external Prometheus servers, administrators must set the exportMetrics flag inside the Prometheus monitoring section of the StorageCluster spec. The correct configuration is:
spec:
monitoring:
prometheus:
exportMetrics: true
This declarative configuration directs Portworx to expose its internal metrics on Prometheus endpoints, allowing external monitoring tools to scrape these metrics for observability, alerting, and dashboarding. The operator-managed Portworx cluster leverages this configuration for integration with cloud-native monitoring stacks, ensuring seamless visibility into cluster health, performance, and resource utilization. Using CLI commands alone is insufficient for operator-managed clusters since they don’t persist settings or integrate with Kubernetes manifests. The official Portworx observability guide and operator documentation endorse this method as the recommended approach for metrics exposure and integration with Prometheus-compatible systems【Pure Storage Portworx Monitoring Guide†source】.

4.What is the primary function of the Portworx OCI monitor pod in a Kubernetes environment?
A. To facilitate the installation of Portworx
B. To monitor the health of Kubernetes nodes
C. To manage Kubernetes network policies
Answer: B
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The Portworx OCI monitor pod primarily monitors the health of Kubernetes nodes within the cluster. It collects telemetry data and status updates about node health, resource availability, and connectivity to ensure the Kubernetes environment hosting Portworx pods remains stable and reliable. This monitoring is vital to detect node failures, performance degradation, or resource bottlenecks early, enabling prompt remedial action. The OCI monitor acts as a specialized component interacting with the Kubernetes

control plane and Portworx services to provide real-time node health insights. This role is distinct from installation facilitation or network policy management, focusing instead on operational observability. Official Portworx operator and observability documentation describe the OCI monitor’s function as critical for node health monitoring and overall cluster reliability within Kubernetes environments running Portworx storage【Pure Storage Portworx Observability Docs†source】.

5.Which command could be used to install Portworx on Kubernetes using the PX-Operator?
A. kubectl apply -f
"https://install.portworx.com/<portworx_version>?operator=true&mc=false&kbver=1.25.0&ns=portworx&b=true&kd=type%3Dgp3%2Csize%3D150&s=%2F%2F22type%3Dgp3%2Csize%3D150&c=px-cluster-0584f7fl-b6be-4608-800c-2ac5fb8069e0&stork=true&csi=true&mon=true&tel=false&st=k8s&promop=true"
B. curl -O px-ag-install.sh -L "https://install.portworx.com/$PXVER/air-gapped?kbver=$KBVER"
C. kubectl apply -f "https://install.portworx.com/<portworx_version>?comp=pxoperator&kbver=<k8s-version>&ns=portworx"
Answer: C
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The officially recommended method to install Portworx with Kubernetes Operator support is using the PX-Operator manifest. This is done by applying the manifest URL with the comp=pxoperator parameter. The command:
kubectl apply -f "https://install.portworx.com/<portworx_version>?comp=pxoperator&kbver=<k8s-version>&ns=portworx"
deploys the Portworx Operator, which manages Portworx lifecycle operations such as installation, upgrades, and configuration changes within the Kubernetes cluster. Specifying the Kubernetes version (kbver) and namespace (ns) ensures compatibility and proper scoping. This operator-centric installation enables more efficient management and automation compared to standalone scripts or manual installations. Portworx official operator installation documentation confirms this approach as the best practice for production deployments, streamlining Portworx management in Kubernetes environments【Pure Storage Portworx Operator Installation Guide†source】.