# **Container security checklist**

* Ensure that the container image is pulled from a trusted and verified source.

**Explanation**: Containers use container images. The developers obtained a container image from an official image registry service.

* Scan the container image.

**Explanation**: Vulnerabilities can exist in container images. Images should be regularly scanned and updated to identify vulnerabilities. The developers performed a vulnerability scan on the container image.

* Patch any vulnerabilities.

**Explanation**: The vulnerability scan reported a kernel-level vulnerability. It should be immediately patched.

* Implement role-based access control (RBAC) and the principle of least privilege.

**Explanation**: All of the developers are using a single Kubernetes service account with unrestricted access. The developers must consider creating roles for users with restricted privileges in order to prevent unauthorized access.