# **Container security checklist**

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

**Explanation**: Containers use container images, which developers get from an official

image registry.

* Container image should be scanned.

**Explanation**: Container images can have vulnerabilities, so they should be scanned and updated regularly. The developers scanned the container image for vulnerabilities.

* Patch any vulnerabilities.

**Explanation**: The scan involved a kernel-level vulnerability and should be patched immediately.

* Role-based access control and the principle of least privilege should be implemented.

**Explanation**: Using a single Kurbenetes service account with unrestricted access is not recommended, roles should be implemented to restrict access.