Free Questions for DCA by go4braindumps

Shared by Frederick on 07-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

You are pulling images from a Docker Trusted Registry installation configured to use self-signed certificates, and this error appears:

'x509: certificate signed by unknown authority'.

You already downloaded the Docker Trusted Registry certificate authority certificate from https://dtr.example.com/ca.

How do you trust it? (Select two.)

Options:

A) Place the certificate in '/etc/docker/dtr/dtr.example.com.crt' and restart the Docker daemon on all cluster nodes.

B) Place the certificate in your OS certificate path, trust the certificate system-wide, and restart the Docker daemon across all cluster nodes.

C) Pass '-trust-certificate ca.crt' to the Docker client.

D) Pass --insecure-registry to the Docker client.

E) Place the certificate in '/etc/docker/certs.d/dtr.example com/ca.crt' on all cluster nodes.

Answer:

D, E

Question 2

A container named 'analytics' that stores results in a volume called 'data' was created.

docker run -d --name=analytics -v data:/data app1

How are the results accessed in 'data' with another container called 'app2'?

Options:

A) docker run -d --name=reports --volume=data app2

B) docker run -d --name=reports --volumes-from=analytics app2

C) docker run -d --name=reports --volume=app1 app2

D) docker run -d --name=reports --mount=app1 app2

Answer:

B

Question 3

The following health check exists in a Dockerfile:

'HEALTCHECK CMD curl --fail http://localhost/health || exit 1'

Which of the following describes its purpose?

Options:

A) Defines the action taken when container health fails, which in this case will kill the container with exit status 1 B. Defines the health check endpoint on the localhost interface for external monitoring tools to monitor the health of the docker engine.

C) Defines the health check endpoint on the local host interface for containers to monitor the health of the docker engine.

D) Defines the health check for the containerized application so that the application health can be monitored by the Docker engine

Answer:

A

Question 4

The following health check exists in a Dockerfile:

'HEALTCHECK CMD curl --fail http://localhost/health || exit 1'

Which of the following describes its purpose?

Options:

A) Defines the action taken when container health fails, which in this case will kill the container with exit status 1 B. Defines the health check endpoint on the localhost interface for external monitoring tools to monitor the health of the docker engine.

C) Defines the health check endpoint on the local host interface for containers to monitor the health of the docker engine.

D) Defines the health check for the containerized application so that the application health can be monitored by the Docker engine

Answer:

A

Question 5

A container named 'analytics' that stores results in a volume called 'data' was created.

docker run -d --name=analytics -v data:/data app1

How are the results accessed in 'data' with another container called 'app2'?

Options:

A) docker run -d --name=reports --volume=data app2

B) docker run -d --name=reports --volumes-from=analytics app2

C) docker run -d --name=reports --volume=app1 app2

D) docker run -d --name=reports --mount=app1 app2

Answer:

B

Question 6

Question Type: MultipleChoice

You are pulling images from a Docker Trusted Registry installation configured to use self-signed certificates, and this error appears:

'x509: certificate signed by unknown authority'.

You already downloaded the Docker Trusted Registry certificate authority certificate from https://dtr.example.com/ca.

How do you trust it? (Select two.)

Options:

A) Place the certificate in '/etc/docker/dtr/dtr.example.com.crt' and restart the Docker daemon on all cluster nodes.

B) Place the certificate in your OS certificate path, trust the certificate system-wide, and restart the Docker daemon across all cluster nodes.

C) Pass '-trust-certificate ca.crt' to the Docker client.

D) Pass --insecure-registry to the Docker client.

E) Place the certificate in '/etc/docker/certs.d/dtr.example com/ca.crt' on all cluster nodes.

Answer:
D, E