Free Questions for 300-910 by go4braindumps

Shared by Joyner on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A security team is running vulnerability scans against a CI/CD pipeline. The reports show that RDBMS secrets were found hardcoded in Ansible scripts. The RDBMS resides in the internal network but is accessible from a jump server that resides in a public network.

If an attacker gains access to the scripts, what is the risk exposure?

Options:

A- The Automation server is at risk of being compromised.

B- The Ansible scripts run through encrypted SSH connections.

C- The internal network is at risk of being compromised.

D- The entire CI/CD-related infrastructure is at risk.

Answer:

C

Explanation:

The internal network is at risk of being compromised if an attacker gains access to the Ansible scripts, as the scripts contain hardcoded secrets for the RDBMS which is accessible from a jump server in a public network. This presents a risk as the secrets can be used to gain access to the RDBMS, and from there, the attacker could potentially gain access to the internal network. Additionally, the entire CI/CD-related infrastructure could be at risk if the attacker is able to gain access to the RDBMS, as they could potentially manipulate the data or scripts in order to cause disruption or damage.

Question 2

Question Type: **MultipleChoice**

What are two testing scenarios of the chaos engineering principle? (Choose two.)

Options:

A- maxing out CPU cores on an Elasticsearch cluster

B- removing all users from a version control system

C- executing routine in driver code to emulate I/O errors

D- blocking developers' building access

E- unplugging a core switch device

Answer:

A, E

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.

```
push_configs.yml content:
- hosts: "{{ CHANGED_HOST }}"
  become: yes
  become_method: enable
  connection: network_cli
  gather_facts: no
  tasks:
    - name: Push the template
      ios_config:
        src: "{{ changed_file }}"

Command:
ansible-playbook push_configs.yml -i
ansible_managed_inventory -e "CHANGED_HOST=${CHANGED_HOST}
CHANGES=${CHANGES}"

Error Message:
"msg": "paramiko: The authenticity of host '[ios-xe-mgmt-
latest.cisco.com]:8181' can't be established.\nThe ssh-rsa
key fingerprint is b'b7e974a8cbf96d464f7be3e12a86d265'."
```


The push_configs.yml playbook returns the error shown.

Which action resolves the error?

Options:

A- Install the Paramiko library on the host that runs Ansible

B- Generate a new SSH key pair and add the public key to the target machine

C- Export the ANSIBLE_HOST_KEY_CHECKING=False variable

D- Comment out the StrictHostKeyChecking=yes line from ansible.cfg

Answer:

D

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit.

```
{
  "_index": "linux-servers",
  "_type": "_doc",
  "_id": "mrZ5OXQBMiQCMA9yzEQ6",
  "_version": 1,
  "_score": null,
  "_source": {
    "message": "<38>Aug 29 12:08:37 centos systemd-logind: Removed session
    19802.",
    "@timestamp": "2020-03-29T09:08:37.280Z",
    "type": "rsyslog",
    "@version": "1",
    "hostname": "vcs.local.lan",
    "host": "172.16.40.168"
  },
  "fields": {
    "@timestamp": [
      "2020-08-29T12:03:37.280Z"
    ]
  },
  "sort": [
    1598692117280
  ]
}
```

The JSON object represents a single entry on a centralized log server, but log data cannot be processed because of the format.

What causes the issue?

Options:

A- A hostgroup must be defined

B- The "_type" must represent the process type

C- The priority of the message must be to the server

D- The process name in the message must be parsed into a field

Answer:

B

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

```
---
apiVersion: v1
kind: Service
metadata:
  name: nginxapp-service
spec:
  ports:
  - port: 80
    name: http-port1
    targetPort: nginx-port
    protocol: TCP
  - port: 8080
    name: http-port2
    targetPort: nginx-port
    protocol: TCP
  selector:
    app: nginxapp
  type: LoadBalancer
```

What are the properties of the load balancer in a Kubernetes environment?

Options:

A- Has exposed ports 80 and 8080 to a private IP address and directs outgoing connections to the port named http-port1

B- Has exposed ports 80 and 8080 to a public IP address and directs incoming connections to the port named nginx-port

C- Forwards incoming traffic from the port named nginx-port to ports 80 and 8080 of nginxapp

D- Forwards any outgoing traffic from the port named nginx-port to exposed ports http-port1 and http-port2 of nginxapp

Answer:

B

Question 6

Question Type: **MultipleChoice**

Which Kubernetes object ensures that each node is limited to running no more than one pod?

Options:

A- UniCast

B- Deployment

C- DaemonSet

D- ReplicaSet

Answer:

C

Question 7

Question Type: MultipleChoice

A three-tier web application must be moved to containers. A webserver is already in place, and the middleware container can talk to a central database server. The hostname of the database server is known, but the name of the middleware server must be provided to the webserver.

In which file should the name of the middleware server be configured?

Options:

A- Docker Service discovery daemon

B- Docker Swarm

C- Docker Compose

D- Dynamic Host Configuration Protocol

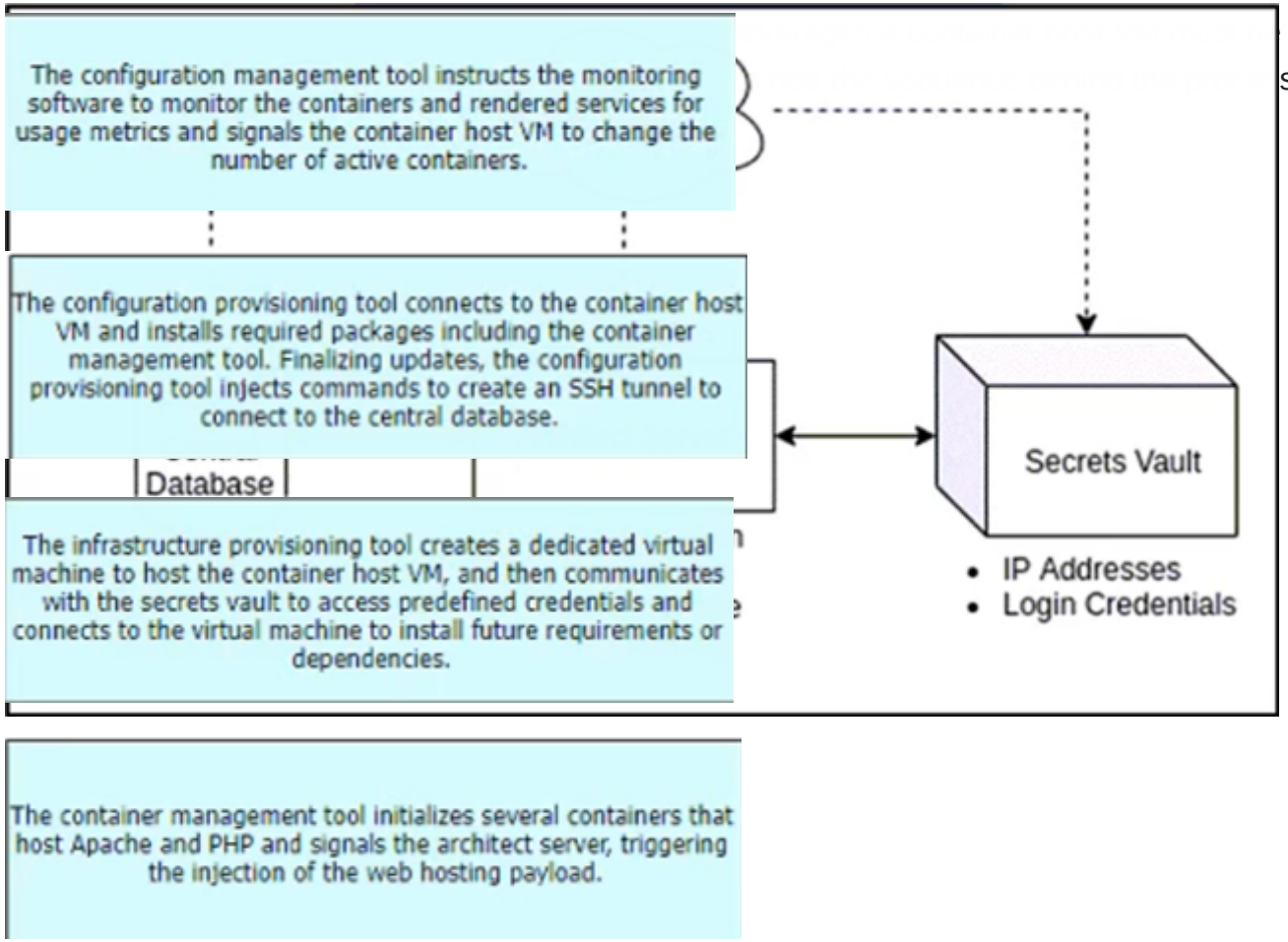
Answer:

A

Question 8

Question Type: **DragDrop**

Refer to the Exhibit.



deployed. Drag and drop the events on the

s.

The configuration management tool instructs the monitoring software to monitor the containers and rendered services for usage metrics and signals the container host VM to change the number of active containers.	step 1
The configuration provisioning tool connects to the container host VM and installs required packages including the container management tool. Finalizing updates, the configuration provisioning tool injects commands to create an SSH tunnel to connect to the central database.	step 2
The configuration provisioning tool creates a dedicated virtual machine to host the container host VM, and then communicates with the secrets vault to access predefined credentials and connects to the virtual machine to install future requirements or dependencies.	step 3
The container management tool initializes several containers that host Apache and PHP and signals the architect server, triggering the injection of the web hosting payload.	step 4

Answer:

Question 9

Question Type: MultipleChoice

Refer to the exhibit.

```
json_data = """
{
  "matchers": [
    {
      "name": "alertname",
      "value": "DevNetExampleAlert",
      "isRegex": false
    },
    {
      "name": "job",
      "value": "core",
      "isRegex": false
    }
  ],
  "startsAt": "2019-07-10T23:42:37.565Z",
  "endsAt": "2019-07-11T01:42:37.565Z",
  "createdBy": "Cisco DevNet",
  "comment": "Silencing this alert while working on it.",
  "id": null
}
"""
```

The snippet contains the JSON string that will be sent to the Prometheus AlertManager to silence an alert. AlertManager accepts only the content type of application 'json" Which Python code correctly sends an API call to perform action?

Options:

A- respone= request.post(url. json=json_data)

B- respone= request.post(url. json=json.loads(json_data)

C- respone= request.post(url. data=json_data)

D- respone= request.post(url, data=json=(json_data)

Answer:

C