300-910Q&As

Implementing DevOps Solutions and Practices using Cisco Platforms (DEVOPS)

Pass Cisco 300-910 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/300-910.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

An end user is seeing long web page load times on the internal business application that they are trying to view. The user is seeing this issue across multiple web browsers, and other users encounter the same issue. Which action should the system administrator take to start looking for the cause of this issue?

A. Check to make sure Nginx is running.

B. Check for response times in Nginx logs.

C. Check to make sure the web API response is coming back in JSON.

D. Check the size of the database that the application is using.

Correct Answer: B

QUESTION 2

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

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

Correct Answer: AE

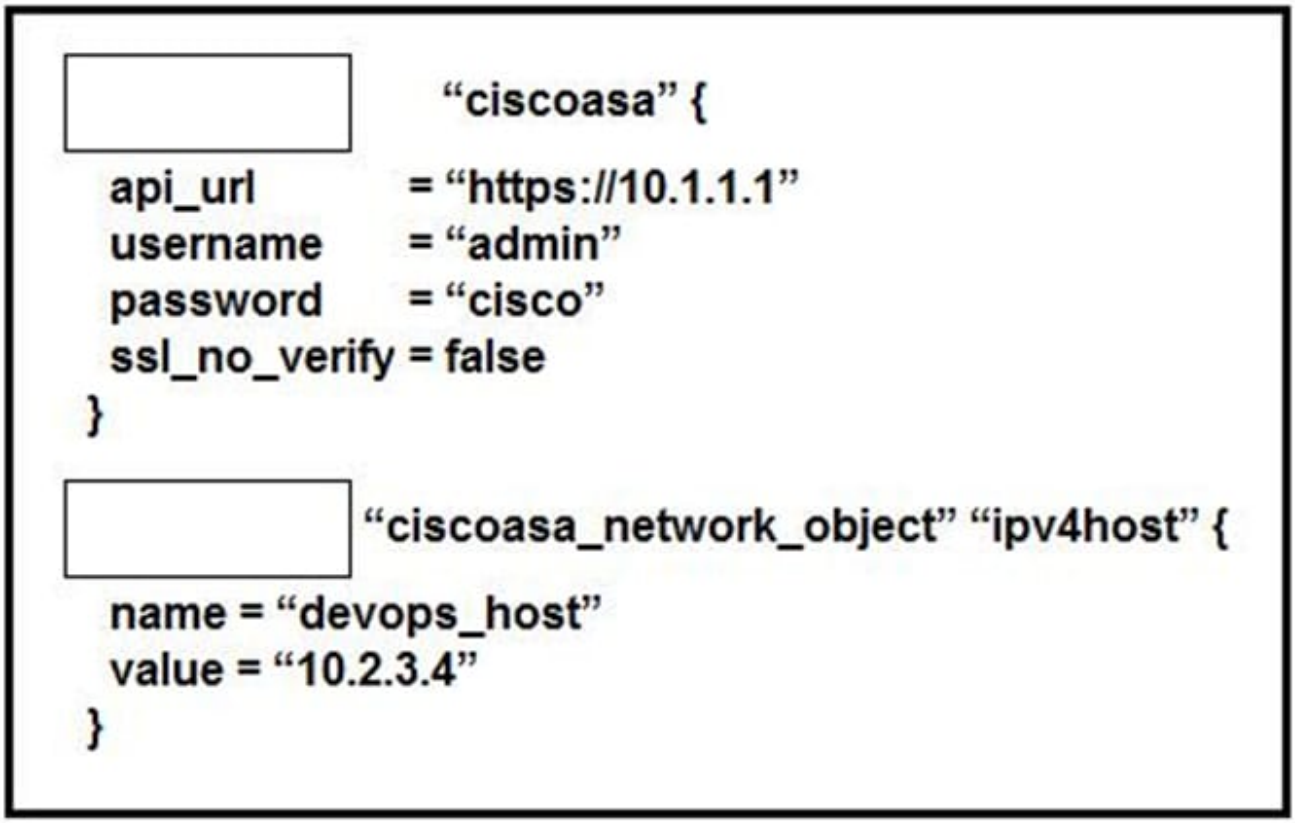
QUESTION 3

DRAG DROP

Drag and drop the commands from the bottom onto the correct Terraform code in the exhibit to push a network object to a Cisco ASA Firewall device.

Select and Place:

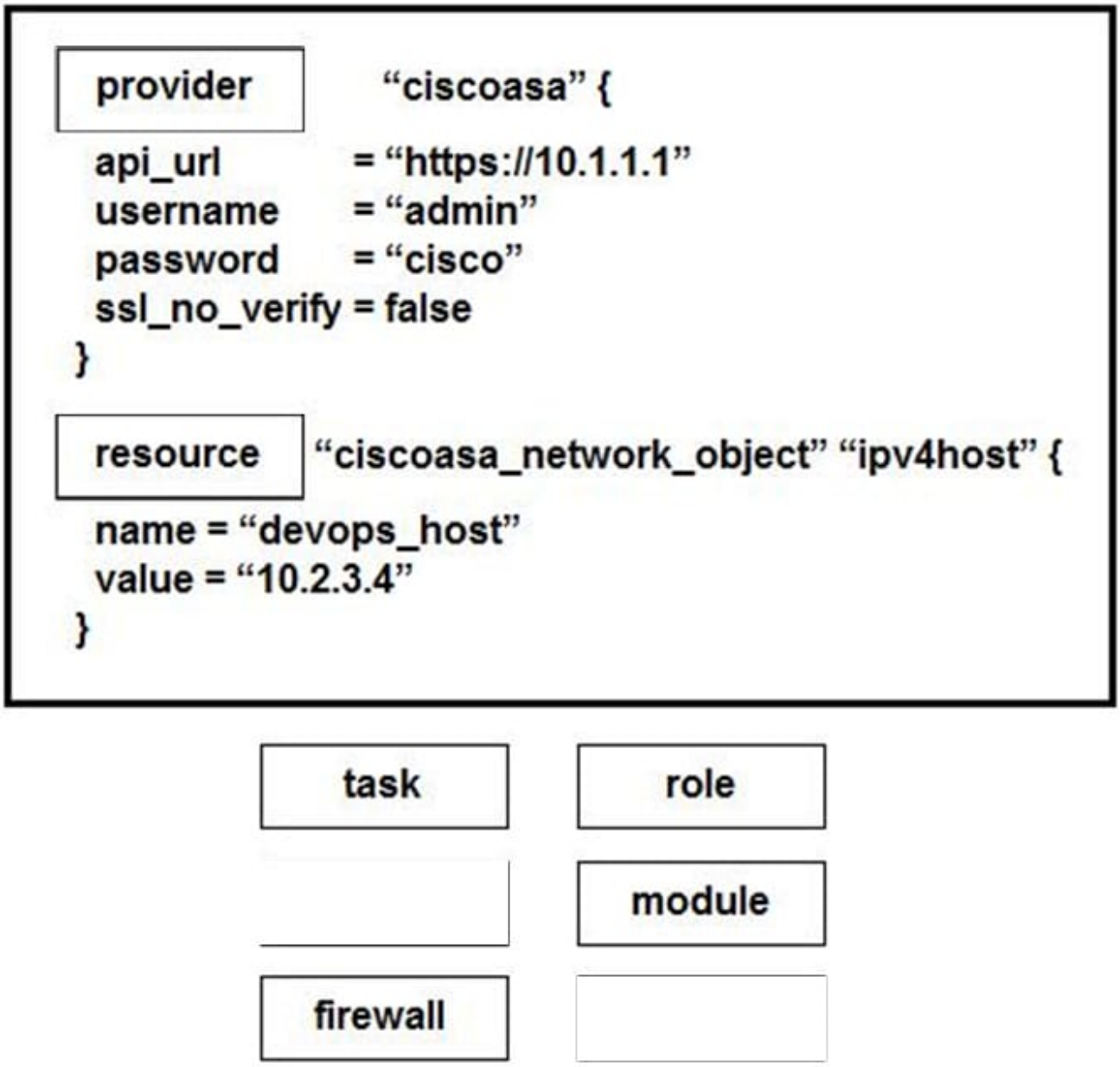
Answer Area



task	role
provider	module
firewall	resource

Correct Answer:

Answer Area



task | role
module
firewall

QUESTION 4

Which two actions help limit the attack surface of your Docker container? (Choose two.)

A. Run only a single service in each container.

B. Run all services in a single image.

C. Use version tags for base images and dependencies.

D. Use Kali Linux as a base image.

E. Download images over HTTPS supporting sites.

Correct Answer: AC

Running only a single service in each container and using version tags for base images and dependencies helps limit the attack surface of your Docker container. This ensures that only the necessary services are running and that you always have the latest versions of the base images and their dependencies, reducing the risk of malicious code being included in the container image. Reference: Docker Documentation, Security Best Practices.

QUESTION 5

How long analysis systems such as Elasticsearch, Logstash, and Kibana Stack handle ingesting unstructured logs from different devices in various formats?

A. All devices that generate syslogs must use agents that process the local logs and transmit them in a specific format to the ELK Stack.

B. All logs are stored in their unstructured text format, and the ELK Stack performs data analysis by intelligently parsing the logs using machine learning algorithms.

C. All different message formats are parsed separately using custom filters, and the resulting structured data is stored for later analysis.

D. A single, comprehensive log format is defined on the ELK Stack. All incoming logs, regardless of format, are transformed to match the comprehensive format, and only applicable fields are populated.

Correct Answer: C

The ELK Stack (Elasticsearch, Logstash, and Kibana) can handle ingesting unstructured logs from various devices in different formats by running custom filters on the logs. The filters are designed to parse the log data and extract the relevant, structured information from it, which is then stored for later analysis. This allows for faster and more accurate analysis of the data, and enables more sophisticated insights to be drawn from it.