Question #1 *Topic 1*

You have deployed a FortiGate HA cluster in Azure using a gateway load balancer for traffic inspection. However, traffic is not being routed correctly through the firewalls.
What can be the cause of the issue?

A. The health probes for the gateway load balancer are failing, which causes traffic to bypass the HA cluster.

B. The protected VMs are in a different Azure subscription, which prevents the gateway load balancer from forwarding traffic.

C. The Fortinet VMs have IP forwarding disabled, which is required for traffic inspection.

D. The gateway load balancer is not associated with the correct network security group (NSG) rules, which allow traffic to pass through.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Your organization has several FortiGate VMs deployed in Azure. You need to implement a solution with Azure native tools that allows you to determine whether packets are being permitted or blocked by the FortiGate VMs.
Which solution can you use to meet these requirements?

A. Insert the VM traffic logs in Azure Sentinel.

B. Install the Azure Monitor agent in all VMs.

C. Use IP flow verify for each of the VMs.

D. Configure Azure Advisor to analyze the network traffic.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

An AWS administrator must ensure that each member of the cloud deployment team has the correct permissions to deploy and manage resources using CloudFormation. The administrator is researching which tasks must be executed with CloudFormation and therefore require CloudFormation permissions.
Which task is run using CloudFormation?

A. Installing a Helm chart to deploy a FortiWeb ingress controller in an EKS cluster

B. Creating an EKS cluster with the eksctl create cluster command

C. Changing the number of nodes in a EKS cluster from AWS CloudShell

D. Deploying a new pod with a service in an Elastic Kubernetes Service (EKS) cluster using the kubectl command

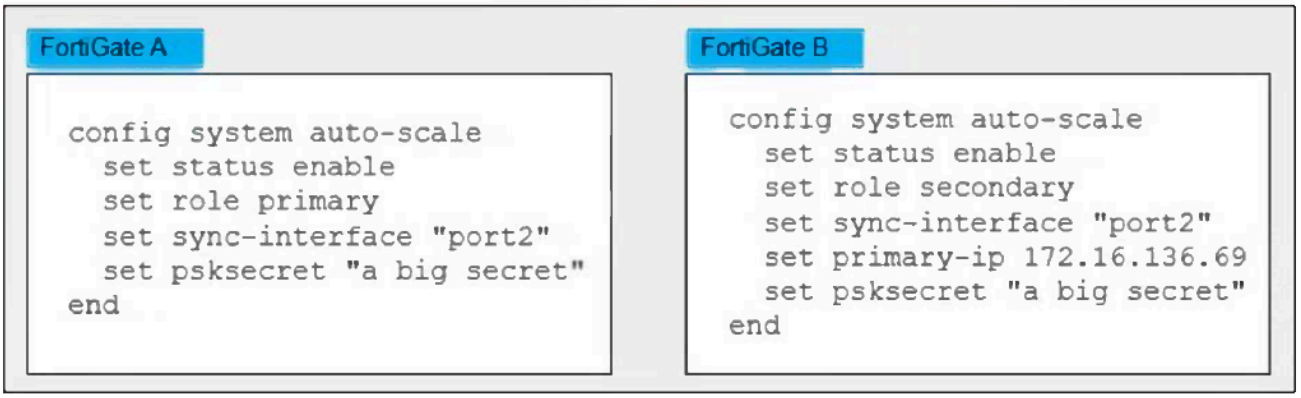
Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Refer to the exhibit.

HA configuration



An administrator deployed an HA active-active load balance sandwich in Microsoft Azure. The setup requires configuration synchronization between devices.

What can you conclude from the configured settings shown in the exhibit? (Choose two.)

A. FortiGate A and FortiGate B are two independent devices.

B. By default, FortiGate uses FGCP.

C. It does not synchronize the FortiGate hostname.

D. FortiGate-VM instances are scaled out automatically according to predefined workload levels.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

A VM in Azure is failing to communicate with other VMs in the same subnet.
What is the most likely cause?

A. Some of the VMs are beyond your allowed quota for the Azure region.

B. There is at least one user-defined route blocking traffic within the subnet.

C. The VMs do not have a public IP address configured.

D. A network security group (NSG) has overridden the default intrasubnet communication rule.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

An Azure administrator is trying to optimize the Azure Bicep files currently used for cloud deployments.
Which technique can Azure administrators use to improve the code in Azure Bicep files?

A. Use the what-if operation before deploying new resources.

B. Avoid nesting related resources to improve readability.

C. Always use parameter files with the .json extension.

D. Limit the allowed parameters with the use of decorators.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

An administrator is looking for a solution that can provide insight into users and data stored in major SaaS applications in the multicloud environment.
Which product should the administrator deploy to have secure access to SaaS applications?

A. FortiSandbox

B. FortiWeb

C. FortiSIEM

D. FortiCASB

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

How does an administrator secure container environments in Amazon AWS from newly emerged security threats?

A. Using Amazon AWS-related application control signatures.

B. Using Docker-related application control signatures.

C. Using distributed network-related application control signatures.

D. Using Amazon AWS_S3-related application control signatures.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

You are automating configuration changes on one of the FortiGate VMs using Linux Red Hat Ansible.
How does Linux Red Hat Ansible connect to FortiGate to make the configuration change?

A. It uses a YAML file.

B. It uses a FortiGate VIP.

C. It uses an API.

D. It uses SSH.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibit.

variable configuration

```
variable access_key {}
variable secret_key {}

variable "region" {
  default = "eu-west-1"
}

// Availability zones for the region
variable "az1" {
  default = "eu-west-1a"
}

variable "vpccidr" {
  default = "10.2.0.0/16"
}

variable "publiccidraz1" {
  default = "10.1.0.0/24"
}

variable "privatecidraz1" {
  default = "10.1.1.0/24"
}

// License Type to create FortiGate-VM
// Provide the license type for FortiGate-VM Instances, either
byol or payg. variable "license_type" {
  default = "byol"
}

// AMIs are for FGTVM-AWS(PAYG) - 7.6.0
variable "fgtvmami" {
```

You are tasked to deploy a FortiGate VM with private and public subnets in Amazon Web Services (AWS). You examined the variables.tf file.
Assume that all the other terraform files are in place.
What will be the final result after running the terraform init and terraform apply commands?

A. Terraform will deploy a FortiGate VM in the eu-West-1 region with private and public subnets.

B. Terraform will deploy a FortiGate VM in the eu-West-1a availability zone without any subnets.

C. Terraform will not deploy a FortiGate VM.

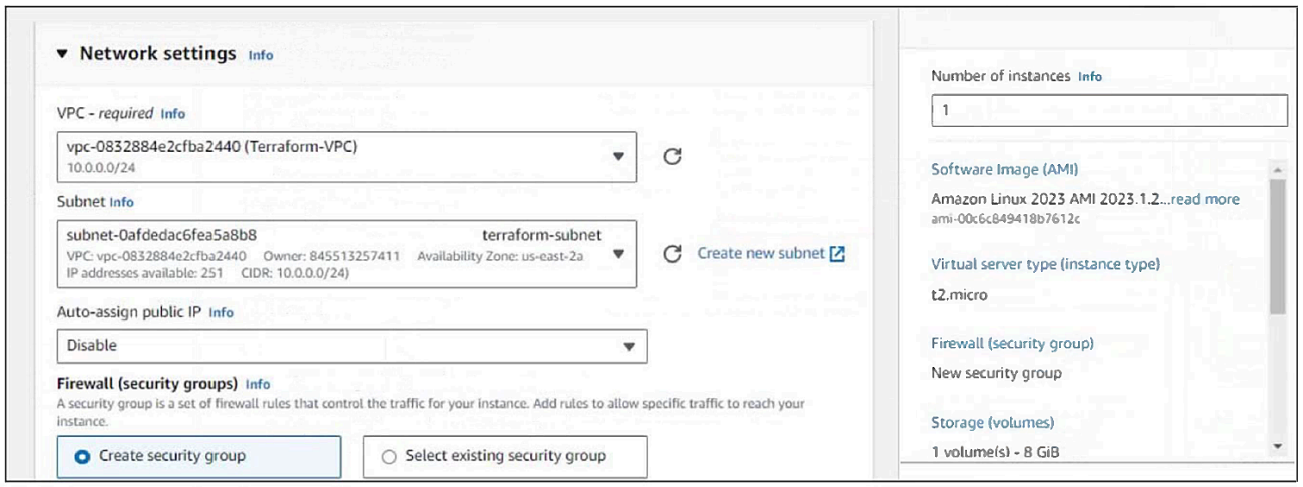
D. Terraform will deploy a FortiGate VM in the eu-West-1a availability zone with two subnets and BYOL license.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Refer to the exhibit.



You have deployed a Linux EC2 instance in Amazon Web Services (AWS) with the settings shown on the exhibit.

What next step must the administrator take to access this instance from the internet?

A. Configure the user name and password.

B. Enable SSH and allocate it to the device.

C. Allocate an Elastic IP address and assign it to the instance.

D. Create a VIP on FortiGate to allow access.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

What are two main features in Amazon Web Services (AWS) network access control lists (NACLs)? (Choose two.)

A. NACLs are tied to an instance.

B. The default NACL is configured to allow all traffic.

C. NACLs are stateless, and inbound and outbound rules are used for traffic filtering.

D. You cannot use NACLs and Security Groups at the same time.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Refer to the exhibit.

```
FGT-AP-SDN-Active #
FGT-AP-SDN-Active # diagnose sniffer packet any "host 76.6  2 and port 443" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 76.6  2 and port 443]
```

An administrator has deployed a FortiGate VM in Amazon Web Services (AWS) and is trying to access it using its public IP address from their local computer. However, the connection is not successful, and at the same time FortiGate is not receiving any HTTPS or SSH traffic to its external interface.

What should the administrator check for possible issue?

A. Check the debug flow for any network ACLs.

B. Check the inbound rules of the security groups.

C. Check the FortiGate firewall policies.

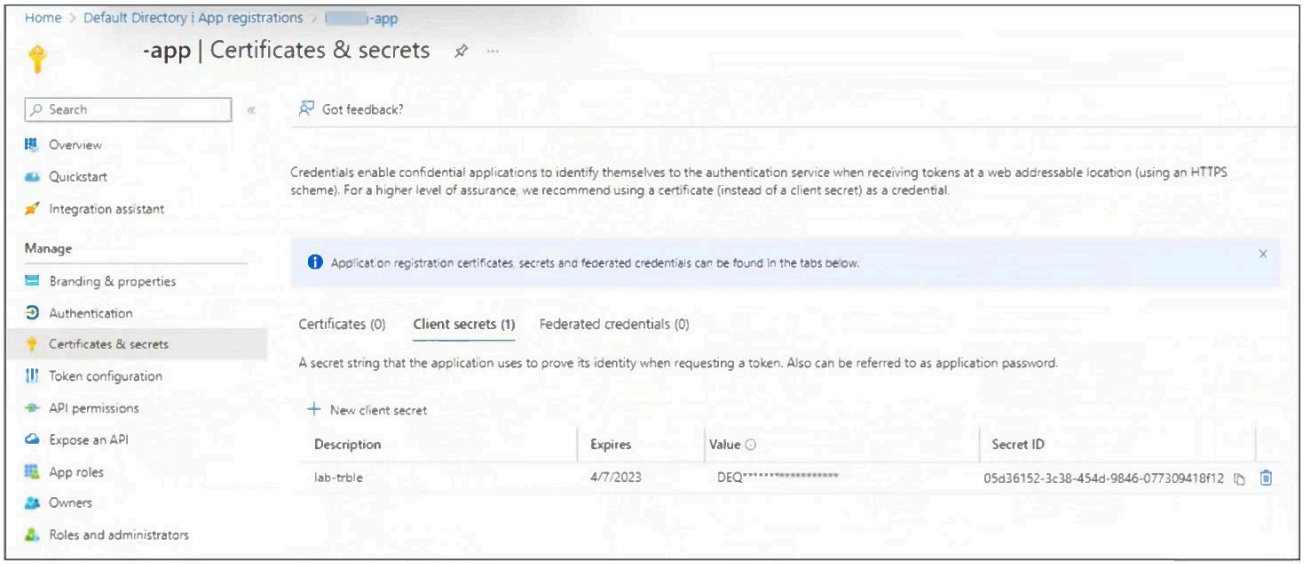
D. Check the FortiGate instance ID.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Refer to the exhibit.



An administrator is trying to deploy a FortiGate VM in Microsoft Azure using Terraform. However, during the configuration, the Azure client secret is no longer visible in the Azure portal.

How would the administrator obtain the Azure client secret to configure on Terraform?

A. Log in to the Azure CLI as a power user to obtain the client secret.

B. Create a new Azure account and assign it the Administrator role.

C. Create a new client secret and take note of it.

D. Use the Terraform output file values to obtain the client secret.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Which statement about immutable infrastructure in automation is true?

A. It is the practice of deploying a new server for every configuration change.

B. It is the practice of deploying two parallel servers for high availability.

C. It is the practice of modifying the existing server configuration after it is deployed.

D. It is the practice of applying hotfixes and OS patches after deployment.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Refer to the exhibit.

HA diagnose output

```
Azure-HA-Passive # diagnose debug application azd -1
Debug messages will be on for 30 minutes.
Azure-HA-Passive # diagnose debug enable
FGT-HA-Slave # azd running in secondary mode, will notupdate
HA event
HA state: primary
azd sdn connector 'AZ-Connector' getting token
size: 1268
token expire in: 3600 seconds
AZ-Connector: resourcegroup: NSE7-HA-RG, sub: "<Removed string>"
Disable interface: port1
Disable interface: port2
get pubip FGTAPClusterPublicIP in resource group NSE7-HA-RG
azd api failed, url
=https://management.azure.com/subscriptions/<Removed String>/resourceGroups/NSE7-HA-
RG/providers/Microsoft.Network/publicIPAddres
ses/FGTAPClusterPublicIP?api-version=2022-06-01, rc = 403,
{"error":{"code":"AuthorizationFailed","message":"The client '<Removed String>' with obj
ect id '<Removed String>' does not have authorization to perform action
'Microsoft.Network/publicIPAddresses/read' over scope '/subscriptions/<Removed
String>/resourceGroups/NSE7-HA-
RG/providers/Microsoft.Network/publicIPAddresses/FGTAPClusterPublicIP' or the scope is
invalid. If access was recen
tly granted, please refresh your credentials."}}
```

You are troubleshooting a FortiGate HA floating IP issue with Microsoft Azure. After the failover, the new primary device does not have the previous primary device floating IP address.
What could be the possible issue with this scenario?

A. FortiGate port4 does not have internet access.

B. A wrong client secret credential is used.

C. The Azure service principal account must have a contributor role.

D. The error is caused by credential time expiration.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Your administrator instructed you to deploy an Azure vWAN solution to create a connection between the main company site and branch sites to the other company VNETs.
What is the best connection solution available between your company headquarters, branch sites, and the Azure vWAN hub?

A. An L2TP connection

B. GRE tunnels

C. SSL VPN connections

D. ExpressRoute

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Refer to the exhibit.

Change set configuration

```
"Changes": [
        {
         "Type": "Resource",
         "ResourceChange": {
           "ResourceType": "AWS::EC2::Instance",
           "LogicalResourceId": "FortiGate_A",
           "PhysicalResourceId": "i0cb1020adr1b308b",
           "Action": "Modify",
           "Replacement": "True",
```

An AWS administrator created a change set to examine the effects of proposed changes to the current infrastructure.
Based on only the output shown in the exhibit, what will happen if the administrator applies these changes?

A. The resulting FortiGate instance will lose its current local users.

B. CloudFormation will roll back the current stack before updating it.

C. The deployment will take place without any service interruption.

D. The PhysicalResourceId will remain the same.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Refer to the exhibit.

what-if tool

```
Resource and property changes are indicated with these symbols:
  - Delete
  + Create
  ~ Modify
The deployment will update the following scope:
Scope: /subscriptions/./resourceGroups/ExampleGroup
~ Microsoft.Network/virtualNetworks/vnet-002 [2018-10-01]
    - tags.Owner: "Production"
    ~ properties.subnets: [
      + 0:
          name:                   "subnet001"
          properties.addressPrefix: "10.0.0.0/25"
]
Resource changes: 1 to modify.
```

An administrator used the what-if tool to preview the changes to an Azure Bicep file.

What will happen if the administrator applies these changes in Azure?

A. The VNet address space will be updated.

B. The resulting VNet will have a single subnet.

C. The vnet-002 VNet will be renamed Production.

D. A new subnet will be added to vnet-002.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Refer to the exhibit.

```
Do you really want to destroy all resources?
 Terraform will destroy all your managed infrastructure, as shown above.
 There is no undo. Only 'yes' will be accepted to confirm.
Enter a value: yes

aws_network_interface_sg_attachment.publicattachment: Destroying... [id=sg-07|
aws_route.externalroute: Destroying... [id=r-rtb-07301520ef1fd3c5c1080289494]
aws_route_table_association.publiclassociate: Destroying... [id=rtbassoc-0142
aws_network_interface_sg_attachment.internalattachment: Destroying... [id=sg-|
aws_eip.FGTPublicIP: Destroying... [id=eipalloc-089e0464d18c2324d]
aws_route_table_association.internalassociate: Destroying... [id=rtbassoc-020
aws_route.internal route: Destroying... [id=r-rtb-0a3d10220e4ed7b221080289494]
aws_route_table_association.publiclassociate: Destruction complete after os
aws_route_table_association.internalassociate: Destruction complete after Os
```

What would be the impact of confirming to delete all the resources in Terraform?

A. It destroys all the resources tied to the AWS Identity and Access Management (IAM) user.

B. It destroys all the resources in the resource group.

C. It destroys all the resources in the state file.

D. It destroys all the resources in the .tfvars file.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Refer to the exhibit.

FortiGate HA configuration

```
config system sdn-connector
    edit "azure-globalsdn-iam-ha"
        set status enable
        set type azure
        set use-metadata-iam enable
        set ha-status enable
        set subscription-id ''
        set resource-group ''
        set azure-region global
        config nic
            edit "fgta-ap-port1"
                config ip
                    edit "ipconfig1"
                        set public-ip "fgt-ap-cluster"
                        set resource-group "fortigate-ha-training"
                    next
                end
            next
        end
        config route-table
            edit "az_spoke1_useast_web"
                set subscription-id "bc0e730b-2345-4c66-9a74-efdfc1xxxxxxx"
                set resource-group "fortigate-ha-training"
                config route
                    edit "default_spoke1_web"
                        set next-hop "10.60.5.4"
                    next
                    edit "az_spoke1_useast_app"
                        set next-hop "10.60.5.4"
                    next
                end
            next
        end
        set update-interval 40
    next
end
```

You deployed a FortiGate HA active-passive cluster in Microsoft Azure.

Which two statements regarding this particular deployment are true? (Choose two.)

A. During a failover, all existing sessions are transferred to the new active FortiGate.

B. There is no SLA for API calls from Microsoft Azure.

C. The configuration does not synchronize between the primary and secondary devices.

D. You can use the vdom-exception command to synchronize the configuration.

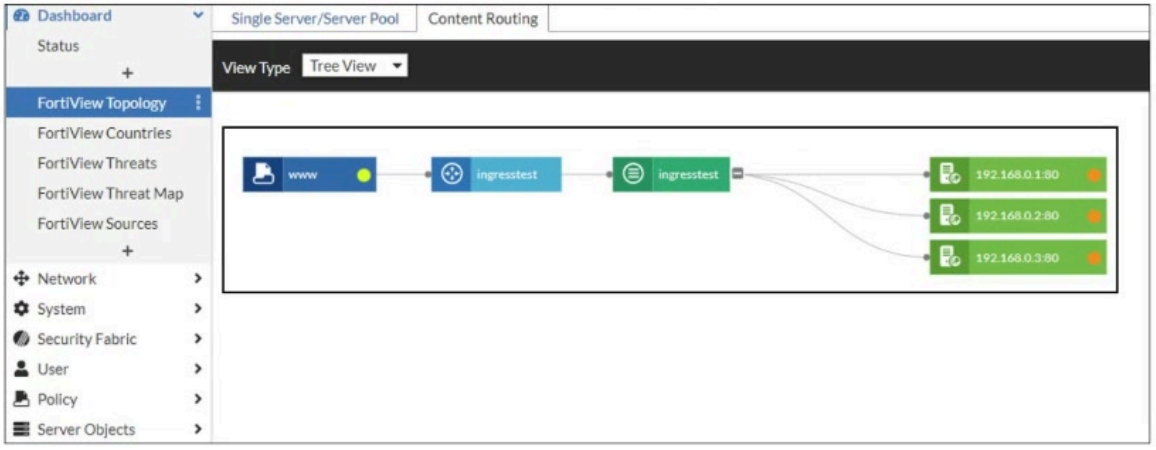
Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Refer to the exhibit.

FortiView Dashboard



An administrator installed a FortiWeb ingress controller to protect a containerized web application.

What is the reason for the status shown in FortiView?

A. The manifest file deployed is configured with the wrong node IP addresses.

B. The FortiWeb VM is missing a route to the node subnet.

C. The load balancing type is not set to round-robin.

D. The SDN connector is not authenticated correctly.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Your DevOps team is evaluating different Infrastructure as Code (IaC) solutions for deploying complex Azure environments.
What is an advantage of choosing Azure Bicep over other IaC tools available?

A. Azure Bicep generates deployment logs that are optimized to improve error handling.

B. Azure Bicep requires less frequent schema updates than Azure Resource Manager (ARM) templates.

C. Azure Bicep can reduce deployment costs by limiting resource utilization during testing.

D. Azure Bicep provides immediate support for all Azure services, including those in preview.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Refer to the exhibit.

Change set configuration


```
"type": "Resource",
    "resourceChange": {
      "action": "Modify",
      "logicalResourceId": "VM1",
      "physicalResourceId": "i-05303cbf3234d1014",
      "resourceType": "AWS::EC2::Instance",
      "replacement": "Conditional",
      "scope": [
        "Properties"
      ],
      "details": [
        {
          "target": {
            "attribute": "Properties",
            "name": "InstanceType",
            "requiresRecreation": "Conditionally",
            "path": "/Properties/InstanceType",
            "beforeValue": "t3.micro",
            "afterValue": "t3.small",
            "attributeChangeType": "Modify"
          },
          "evaluation": "Dynamic",
          "changeSource": "DirectModification"
        },
```


The exhibit shows partial output of changes that AWS found after you created a new change set.

What can you conclude from this output if you decide to execute this change set?

A. CloudFormation will check your account quota before executing the change set, to prevent errors.

B. Resources deployed successfully will remain, even if other resources fail during execution.

C. You should refer to the AWS documentation to prevent unplanned service interruptions.

D. Executing this change set will create a new VM, unless you do not have proper permissions.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

You are experiencing intermittent connectivity issues in a FortiGate HA cluster deployed with Azure gateway load balancer. Traffic is being dropped when it passes through the cluster.
What is the cause of the issue?

A. The Azure gateway load balancer is blocking large packets, causing traffic failures.

B. The protected VMs are running an application that fragments packets.

C. The Azure gateway load balancer is configured with an incorrect health probe port.

D. The FortiGate firewalls are using the default maximum transmission unit (MTU) size supported by Azure.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

Refer to the exhibit.

```
AWSTemplateFormatVersion: "2010-09-09"
Resources:
 FortiGateActive:
   Type: "AWS::EC2::Instance"
   Properties:
    ImageId: "ami-01bd410bcaa617f44"
    InstanceType: t2.large
```

A senior administrator in a multinational organization needs to include a comment in the template shown in the exhibit to ensure that administrators from other regions change the EC2 instance size value to one that meets the requirements in their local deployments. How can the administrator add the comment in that section of the file?

A. The administrator can add the comment with the # character next to the InstanceType section.

B. The administrator must update the AWSTemplateFormatVersion to a more current version.

C. The administrator must convert the template to JSON format before adding the comment.

D. The administrator can run the aws cloudformation update-stack and include the comment.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Refer to the exhibit.

Manifest file

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: simple-fanout-example
  annotations: {
    "fortiweb-ip" : "172.16.0.215",
    "fortiweb-login' :  ??????    ,
    "fortiweb-port" : "8443",
    "fortiweb-ctrl-log" : "disable",
    "virtual-server-ip" : "172.16.0.153",
    "virtual-server-addr-type" : "ipv4",
    "virtual-server-interface" : "port1",
    "server-policy-web-protection-profile" : "Inline Standard Protection",
    "server-policy-https-service" : "HTTPS",
    "server-policy-http-service" : "HTTP",
    "server-policy-syn-cookie" : "enable",
    "server-policy-http-to-https" : "disable"
  }
spec:
  ingressClassName: fwb-ingress-controller
  rules:
  - host: training.fortinet.lab
    http:
      paths:
      - path: /info
        pathType: Prefix
        backend:
          service:
            name: service1
            port:
              number: 1241
```

A team of AWS administrators is in the process of installing a FortiWeb ingress controller to protect containerized web applications in an Amazon Elastic Kubernetes Service (EKS) cluster. While customizing the manifest file in the image, they realize that they do not know the correct value to enter in the fortiweb-login field.

How can they determine he correct value for this field?

A. They can refer to the output of the EKS cluster deployment.

B. They can find the expected value in the manifest file used to deploy the pods.

C. They must create a Kubernetes secret with the kubectl command.

D. The correct value is the password of the FortiWeb admin account.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

A Network security administrator is searching for a solution to secure traffic going in and out of the container infrastructure.
In which two ways can Fortinet container security help secure container infrastructures? (Choose two.)

A. FortiGate NGFW can inspect north-south container traffic with label aware policies.

B. FortiGate NGFW can be placed between each application container for north-south traffic inspection.

C. FortiGate NGFW can connect to the worker nodes and protect the containers.

D. FortiGate NGFW and FortiWeb can be used to secure container traffic.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

An administrator is relying on Azure Bicep linter to find possible issues in Bicep files.
Which problem can the administrator expect to find?

A. Missing dependencies among resources that could cause failures

B. Code issues such as unused parameters or variables

C. Conflicts with the Azure policy for resource configurations

D. Region-specific SKU availability for objects included in the code

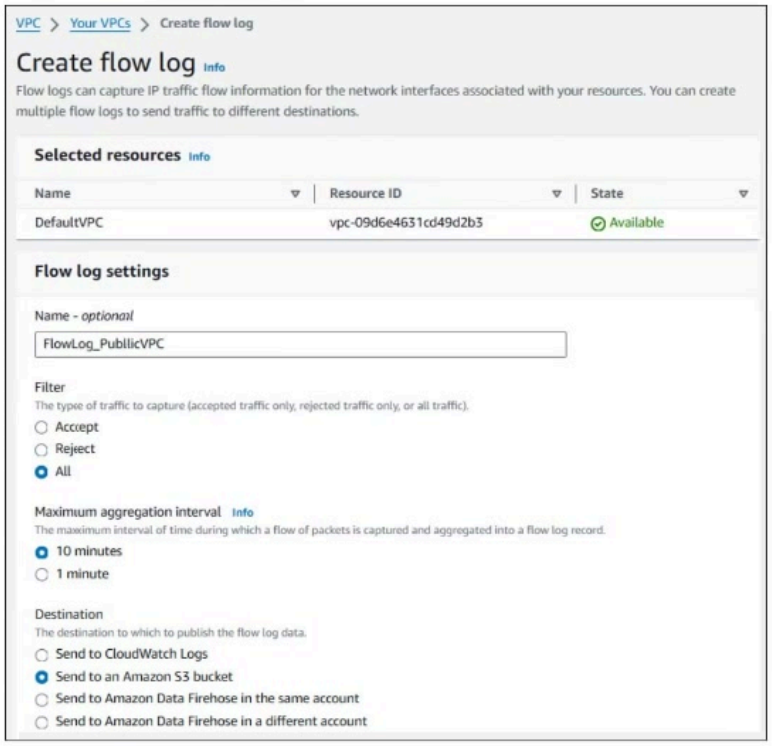
Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Refer to the exhibit.

VPC flow log wizard



Your team notices an unusually high volume of traffic sourced at one of the organizations FortiGate EC2 instances. They create a flow log to obtain and analyze detailed information about this traffic. However, when they checked the log, they found that it included traffic that was not associated with the FortiGate instance in question.

What can they do to obtain the correct logs?

A. Change the maximum aggregation time to 1 minute.

B. Send the logs to Amazon Data Firehose instead to get more granular information.

C. Ensure that the flow log data is not mixed with the rest of the traffic.

D. Create a new flow log at the interface level.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

A customer would like to use FortiGate fabric integration with FortiCNP.
When adding a FortiGate VM to FortiCNP, which three mandatory configuration steps must you follow on FortiGate? (Choose three.)

A. Create an SSL/SSH inspection profile.

B. Configure FortiGate to send logs to FortiCNP.

C. Import the FortiGate certificate into FortiCNP.

D. Enable pre-shared key on both sides.

E. Create and IPS sensor and a firewall policy.

Suggested Answer: *BCD*

Community vote distribution

ABE (100%)

Airness 3 months, 2 weeks ago

Selected Answer: ABE

https://docs.fortinet.com/document/forticnp/22.4.a/online-help/628651/fortigate-fabric-integration

upvoted 1 times

Question #32 *Topic 1*

You are troubleshooting a FortiGate active-passive SDN connector solution in Microsoft Azure.
Which two mandatory SDN connector settings are required for a successful deployment? (Choose two.)

A. FortiGate license file

B. Client secret

C. Active FortiGate serial number

D. Directory ID

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

An administrator is trying to implement FortiCNP with Microsoft Azure Security integration. However, FortiCNP is not able to extract any cloud integration data from Azure; therefore, real-time cloud security monitoring is not possible.
What is causing this issue?

A. The FortiCNP account in Azure has the Storage Blob Data Reader role.

B. The organization is using a free Azure AD license.

C. The administrator enabled the wrong defender plan for servers.

D. The Azure account doesn't have the global administrator role.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!