Comptia

CV0-002
CompTIA Cloud+ Exam

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ **Up to Date products, reliable and verified.**
✓ **Questions and Answers in PDF Format.**

Latest Version: 15.0

Question: 1

A new browser version has been deployed to all users at a company. After the deployment, users report that they can no longer access the company's secure time-card system, which is hosted by a SaaS provider. A technician investigates and discovers a security error is received upon opening the site. If the browser is rolled back to the older version, the site is accessible again. Which of the following is the MOST likely cause of the security error users are seeing?

A. SSL certificate expiration on the SaaS load balancers
B. Federation issues between the SaaS provider and the company
C. Obsolete security technologies implemented on the SaaS servers
D. Unencrypted communications between the users and the application

Answer: C

Question: 2

A company has decided to scale its e-commerce application from its corporate datacenter to a commercial cloud provider to meet an anticipated increase in demand during an upcoming holiday. The majority of the application load takes place on the application server under normal conditions. For this reason, the company decides to deploy additional application servers into a commercial cloud provider using the on-premises orchestration engine that installs and configures common software and network configurations. The remote computing environment is connected to the on-premises datacenter via a site-to-site IPSec tunnel. The external DNS provider has been configured to use weighted round-robin routing to load balance connections from the Internet.
During testing, the company discovers that only 20% of connections completed successfully.
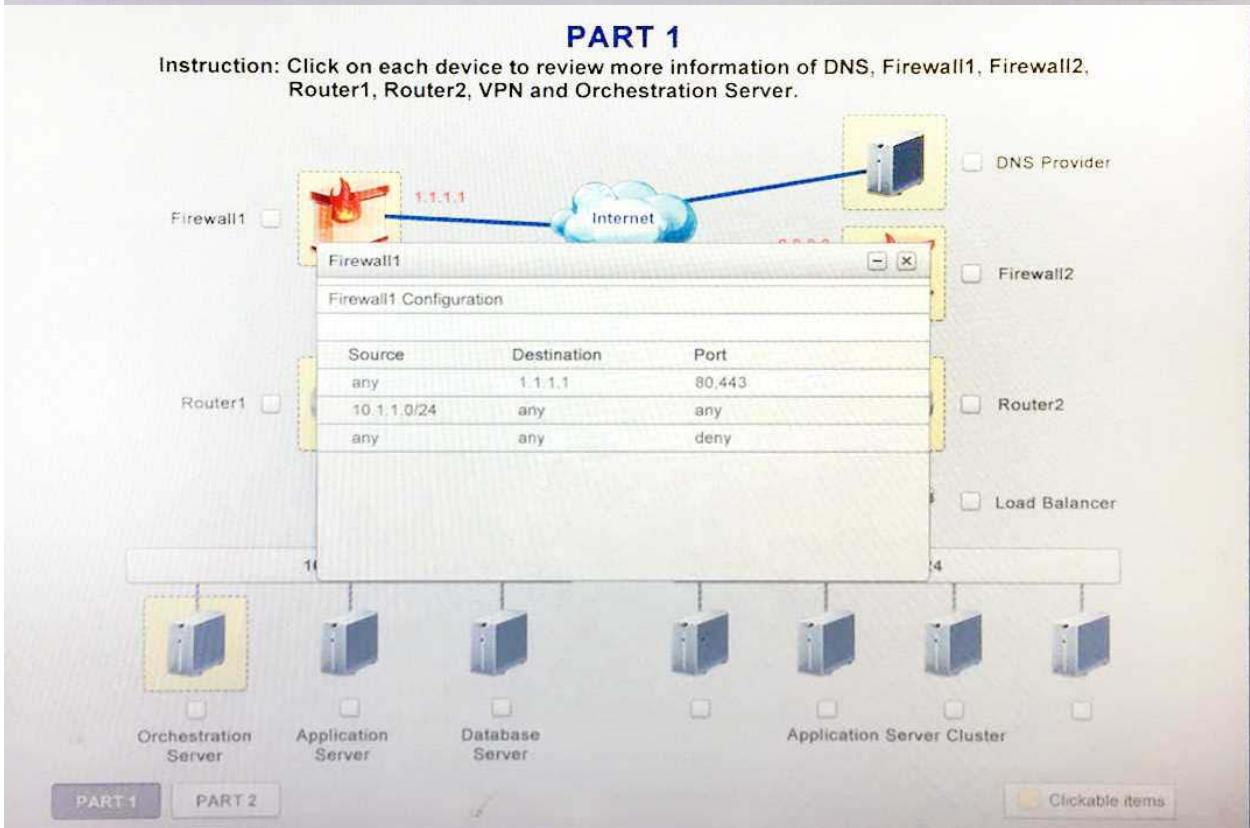Review the network architecture and supporting documents and fulfill these requirements:
Part1:
1. Analyze the configuration of the following components: DNS, Firewall1, Firewall2, Router1, Rouler2, VPN and Orchestrator Server.
2. Identify the problematic device(s).
Instructions:
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.
Simulation

PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.

Firewall1 — 1.1.1.1 — Internet — DNS Provider

2.2.2.2 — Firewall2

Site-to-Site IPSec Tunnel

Router1 — Router2

Load Balancer

10.1.1.0 / 24   10.1.2.0 / 24

Orchestration Server — Application Server — Database Server — Application Server Cluster

PART 1   PART 2   Clickable items

PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.

Firewall1 — 1.1.1.1 — Internet — DNS Provider

Firewall2

Firewall1   — [×]

Firewall1 Configuration

Source	Destination	Port
any	1.1.1.1	80,443
10.1.1.0/24	any	any
any	any	deny

Router1   Router2

Load Balancer

Orchestration Server — Application Server — Database Server — Application Server Cluster

PART 1   PART 2   Clickable items

PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2. Router1, Router2, VPN and Orchestration Server.

DNS Provider

Firewall1

Internet

Router1	□	×

Router1 Configuration

Public IP: 1.1.1.1

Internal IP: 10.1.1.1/24

Firewall2

Site-to-Site VPN Configuration

Address Space: 10.1.1.0/24

Router1

Subnet: 255.255.255.0

Router2

PSK: Cloud001

IKE: SHA1/AES256/DH2/SA Lifetime: 28800

Load Balancer

1   4

Orchestration Server   Application Server   Database Server   Application Server Cluster

PART 1   PART 2   Clickable items

PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2. Router1, Router2, VPN and Orchestration Server.

DNS Provider

Firewall1

1.1.1.1

Internet

DNS			□ ×

Firewall2

Name	Type	Value	Weight
www.mycorp.com	CNAME	onprem.mycorp.com	20%
www.mycorp.com	CNAME	cloud.mycorp.com	80%
onprem.mycorp.com	A	1.1.1.1	-
cloud.mycorp.com	A	2.2.2.2	-

Router1

Router2

Load Balancer

1   4

Orchestration Server   Application Server   Database Server   Application Server Cluster

PART 1   PART 2   Clickable items

PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.

☐ DNS Provider

Firewall1 ☐

1.1.1.1

Internet

☐ Firewall2

Firewall2

Firewall2 Configuration

Source	Destination	Port
any	2.2.2.2	80 443
10 1 2 0/24	any	any
any	any	deny

Router1 ☐

☐ Router2

☐ Load Balancer

Orchestration Server   Application Server   Database Server   Application Server Cluster

PART 1   PART 2

Clickable items

PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.
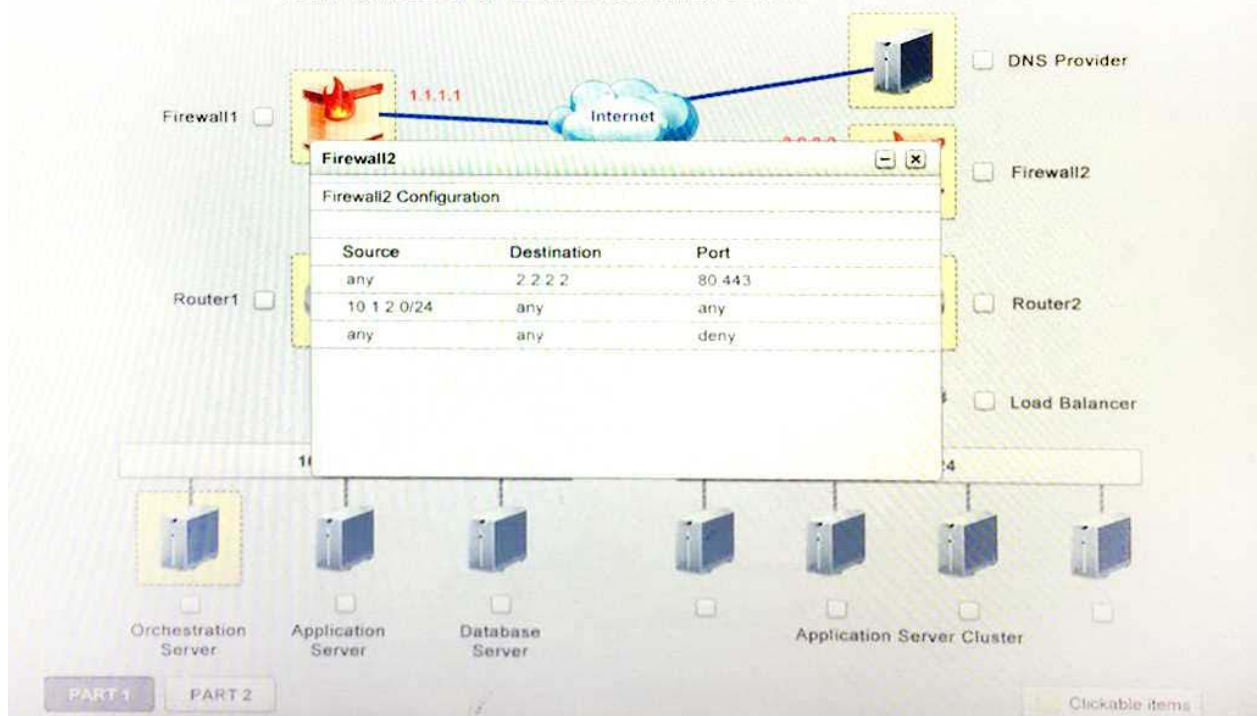
Firewall1

1.1.1.1

Internet

DNS Provider

Router2 ⊟ ⊠

Router2 Configuration

Public IP: 2.2.2.2

Internal IP: 10.1.2.1/24

Firewall2

Site-to-Site VPN Configuration

Router1

Address Space: 10.1.1.0/24

Subnet: 255.255.255.0

PSK: Cloud002

IKE: SHA1/AES256/DH2/SA Lifetime: 28800

Router2

Load Balancer

Orchestration Server

Application Server

Database Server

Application Server Cluster

PART 1   PART 2

PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.

Firewall1   1.1.1.1   Internet   DNS Provider

VPN   [–] [x]

Site-to-Site VPN Configuration

PSK: Cloud001

IKE: SHA1/AES256/DH2/SA Lifetime. 28800

Firewall2

Router1   Router2

Load Balancer

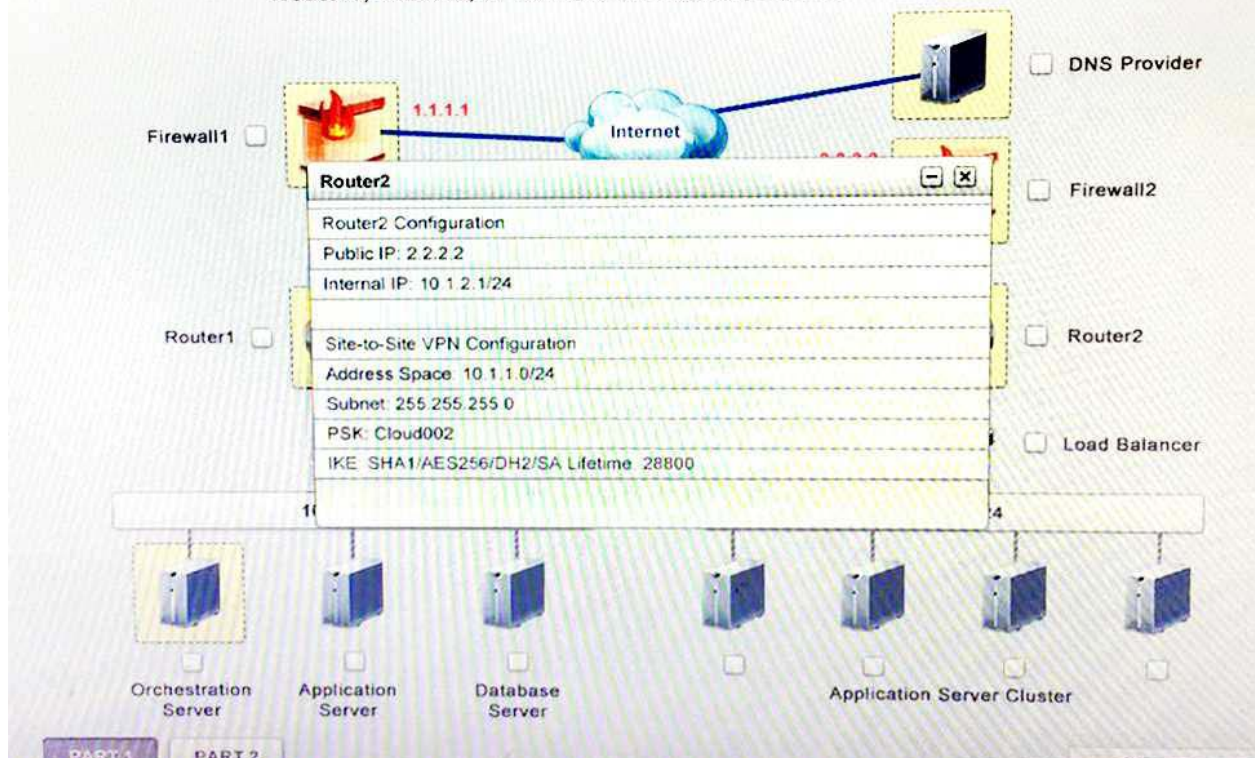Orchestration Server   Application Server   Database Server   Application Server Cluster

PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.
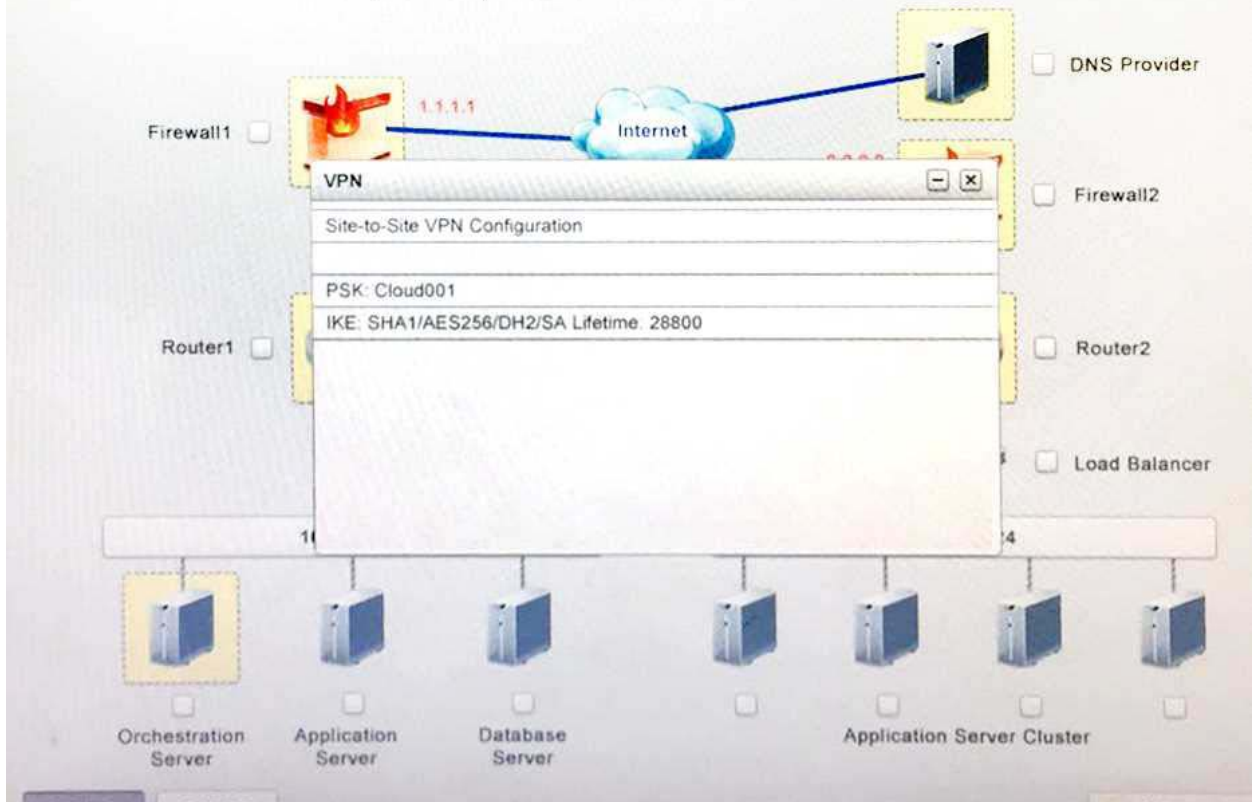
DNS Provider

Firewall1   1.1.1.1   Internet

Orchestration Server   — ×

Name: Basic_Server
Network: 10.1.1.0/24

Name: Cloud_Server
Network: 10.1.2.0/24

Name: Application_Server
Baseline: Basic_Server
Type: Webserver
Version: 1.0

Firewall2

Router1

Router2

Load Balancer

Orchestration Server   Application Server   Database Server   Application Server Cluster

PART 1   PART 2   Clickable items

Router1, Router2, VPN and Orchestration Server.

DNS Provider

Firewall1   1.1.1.1   Internet

Orchestration Server   — ×

Baseline: Basic_Server
Type: Webserver
Version: 1.0

Name: Database_Server
Baseline: Basic_Server
Type: Database Server
Verson: 1.0

Name: Corporate_Datacenter
Baseline: Application_Server

Firewall2

Router2

Load Balancer

Orchestration Server   Application Server   Database Server   Application Server Cluster

PART 1   PART 2

Question

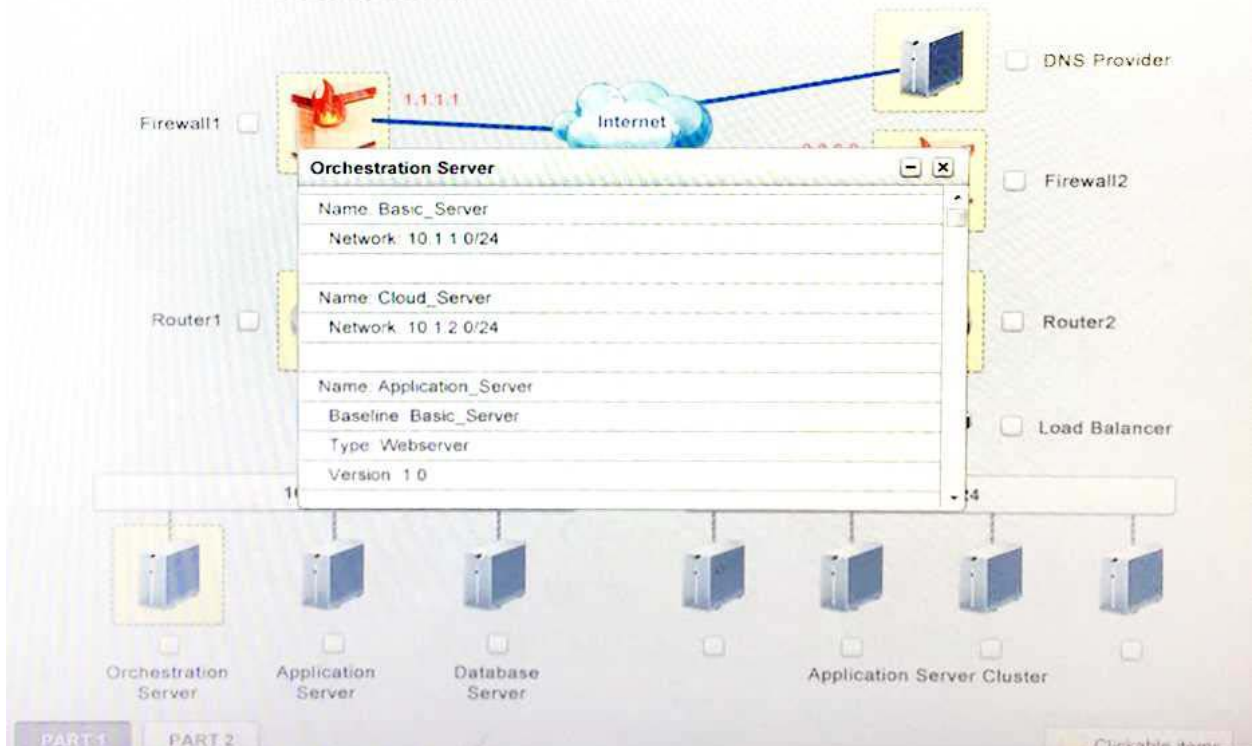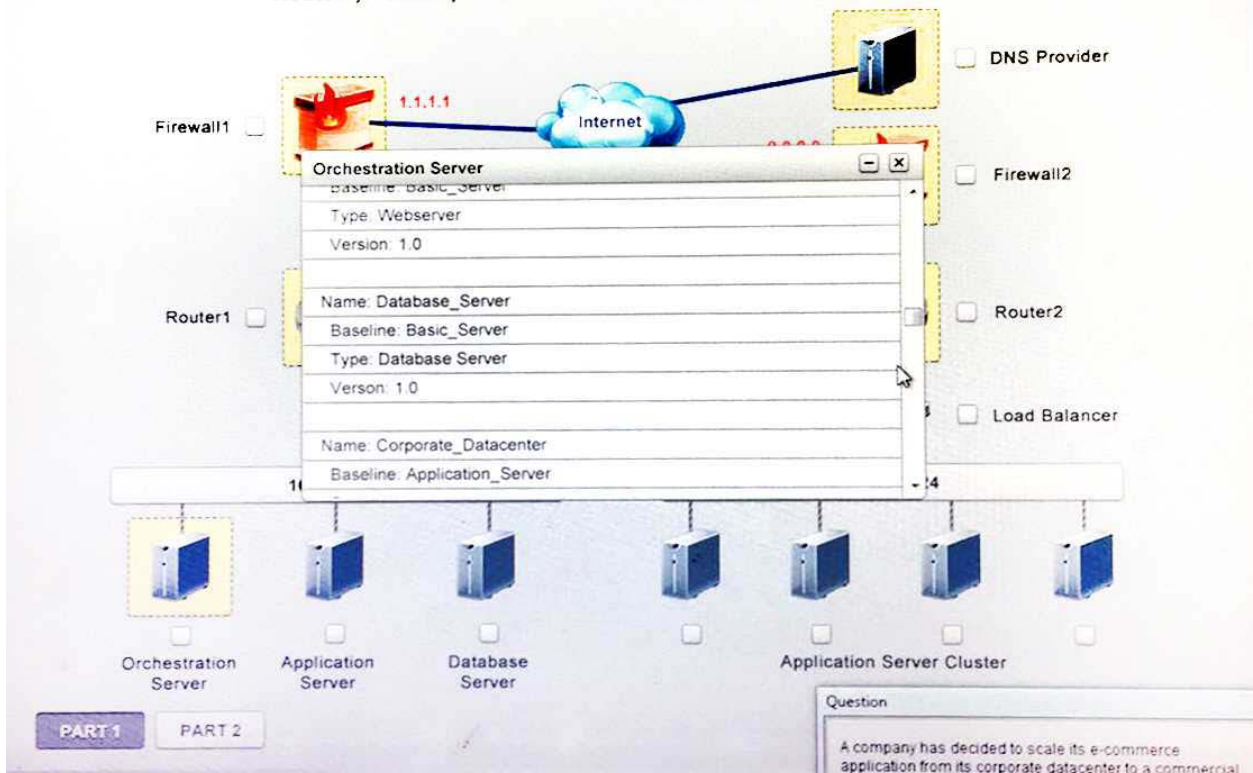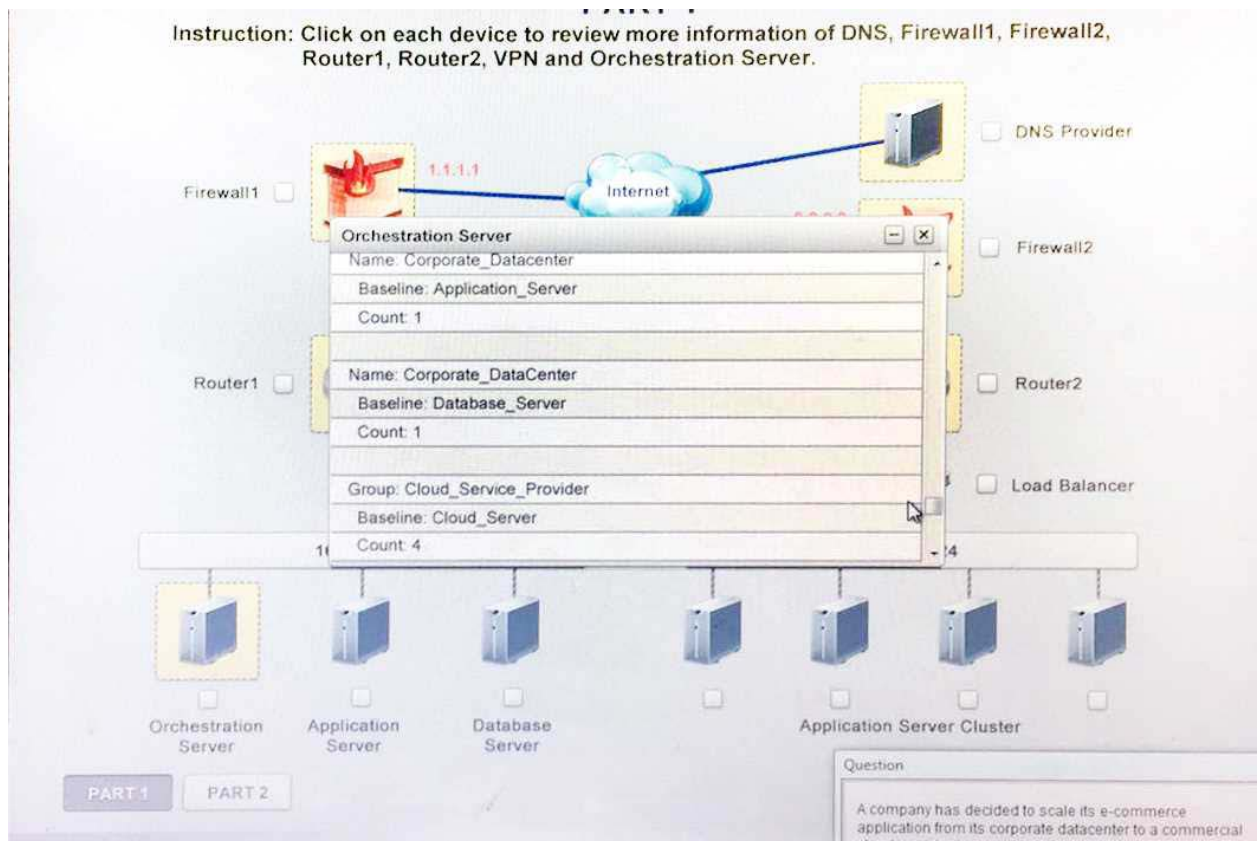A company has decided to scale its e-commerce application from its corporate datacenter to a commercial

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2,
Router1, Router2, VPN and Orchestration Server.

Firewall1

1.1.1.1

Internet

DNS Provider

Orchestration Server

Name: Corporate_Datacenter
Baseline: Application_Server
Count: 1

Name: Corporate_DataCenter
Baseline: Database_Server
Count: 1

Group: Cloud_Service_Provider
Baseline: Cloud_Server
Count: 4

Firewall2

Router1

Router2

Load Balancer

Orchestration
Server

Application
Server

Database
Server

Application Server Cluster

PART 1   PART 2

Question

A company has decided to scale its e-commerce
application from its corporate datacenter to a commercial
cloud provider to meet an anticipated increase in demand

Answer: See the solution below.

Solution given below with details.

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.

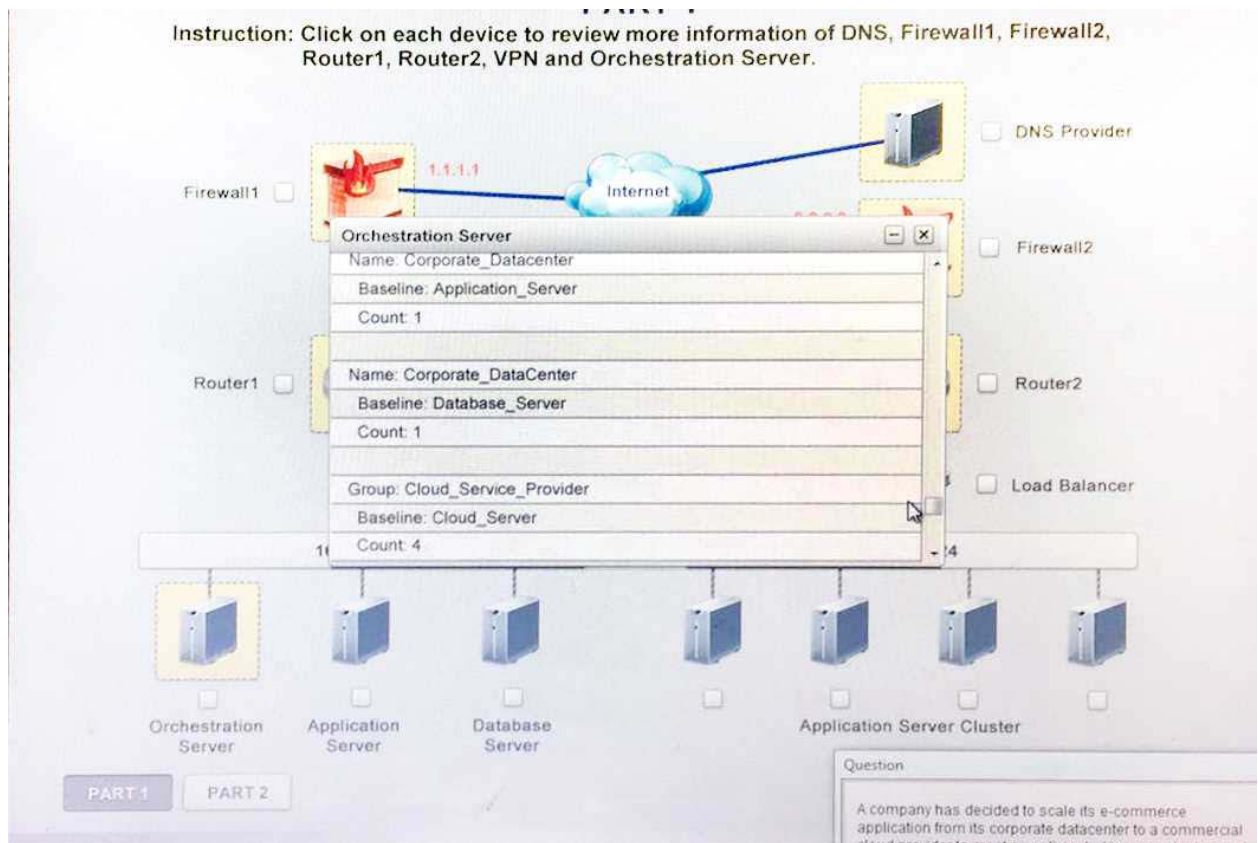Orchestration Server

Name: Corporate_Datacenter
Baseline: Application_Server
Count: 1

Name: Corporate_DataCenter
Baseline: Database_Server
Count: 1

Group: Cloud_Service_Provider
Baseline: Cloud_Server
Count: 4

DNS Provider

Firewall1

Firewall2

Router1

Router2

Load Balancer

Orchestration Server   Application Server   Database Server   Application Server Cluster

PART 1   PART 2

Question

A company has decided to scale its e-commerce application from its corporate datacenter to a commercial cloud provider to meet an anticipated increase in demand

Question: 3

DRAG DROP
A hosted file share was infected with CryptoLocker and now root cause analysis needs to be performed. Place the tasks in the correct order according to the troubleshooting methodology.

#		Task
1		Establish a plan of action to resolve the problem and implement remediation
2		Establish a theory of probable cause
3		Document findings and outcomes
4		Identify the problem
5		Test the theory to determine cause
6		Verify full system functionality

1	Identify the problem	Establish a plan of action to resolve the problem and implement remediation	
2	Establish a theory of probable cause	Establish a theory of probable cause	
3	Test the theory to determine cause	Document findings and outcomes	
4	Establish a plan of action to resolve the problem and implement remediation	Identify the problem	
5	Verify full system functionality	Test the theory to determine cause	
6	Document findings and outcomes	Verify full system functionality	

Question: 4

A company is seeking a new backup solution for its virtualized file servers that fits the following characteristics:
The files stored on the servers are extremely large.
Existing files receive multiple small changes per day.
New files are only created once per month.
All backups are being sent to a cloud repository.
Which of the following would BEST minimize backup size?

A. Local snapshots
B. Differential backups
C. File-based replication
D. Change block tracking

Answer: B

Reference: https://www.acronis.com/en-us/blog/posts/tips-tricks-better-business-backup-and-recoveryworld-backup-day

Question: 5

A company has deployed a four-node cluster in a COLO environment with server configurations listed below. The company wants to ensure there is 50% overhead for failover and redundancy. There are currently eight VMs running within the cluster with four vCPUs x32GB each. The company wants to better utilize its resources within the cluster without compromising failover and redundancy.

White Label Servers	Configuration (CPU x Memory GB)
Server 1	16x128
Server 2	16x128
Server 3	16x128
Server 4	16x128

Given the information above, which of the following should a cloud administrator do to BEST accommodate failover and redundancy requirements?

A. Ensure hyperthreading is being utilized with physical server CPUs.
B. Ensure dynamic resource allocation is being utilized.
C. Overcommit memory, and the systems will allocate resources as required.
D. Set hard limits for VM resources and turn on hyperthreading.

Answer: B

Thank You for Trying Our Product

Discount Coupon Code:

EXAMSBOOST10

For More Information – **Visit link below:**

http://www.examsboost.com/

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**