Pass4IT

CompTIA
CV0-003

QUESTIONS AND ANSWERS

FREE VERSION

(LIMITED CONTENT)

Dumps Questions CV0-002

Exam Name: CompTIA Cloud+ (CV0-002)

Certification Provider: CompTIA

Exam: CompTIA Cloud+ (CV0-002)

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

Correct Answer: C

Question #2

SIMULATION -
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.
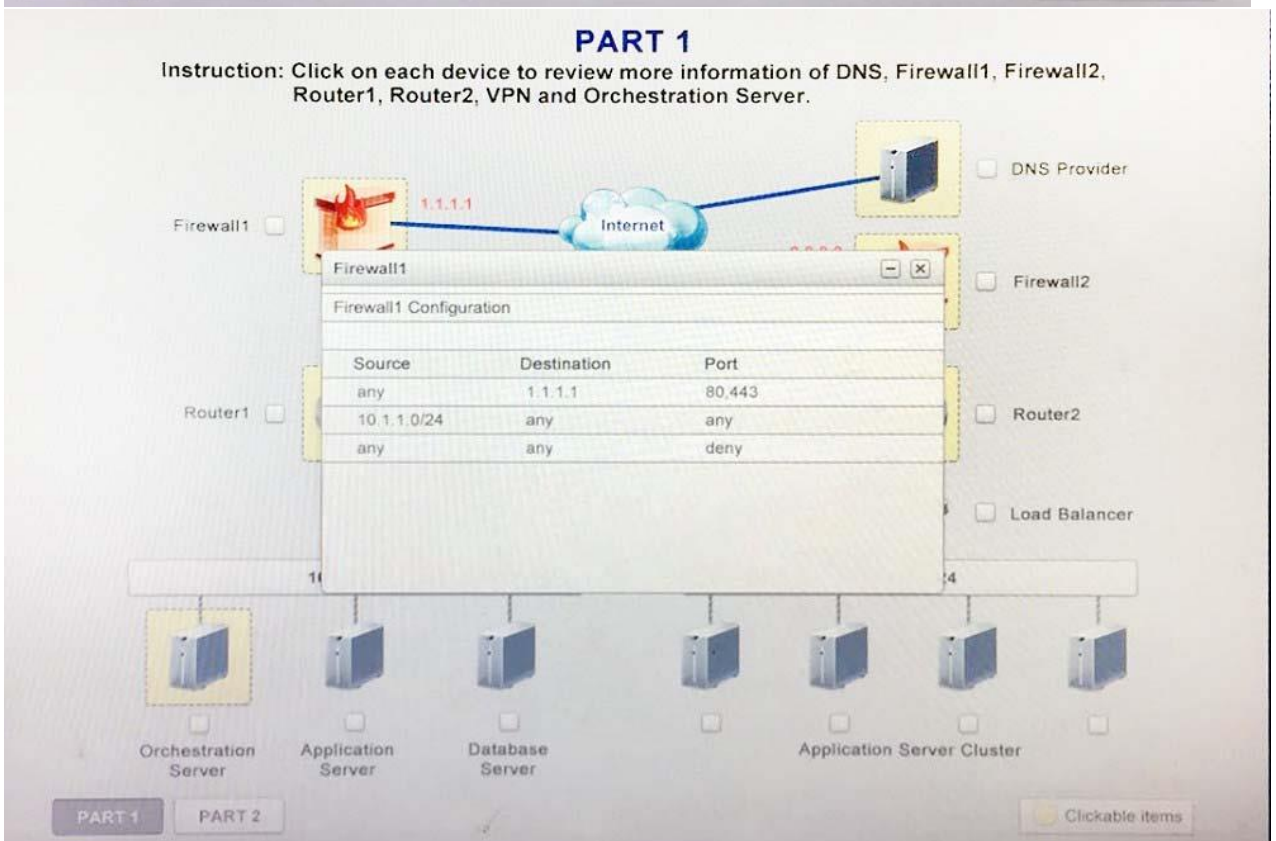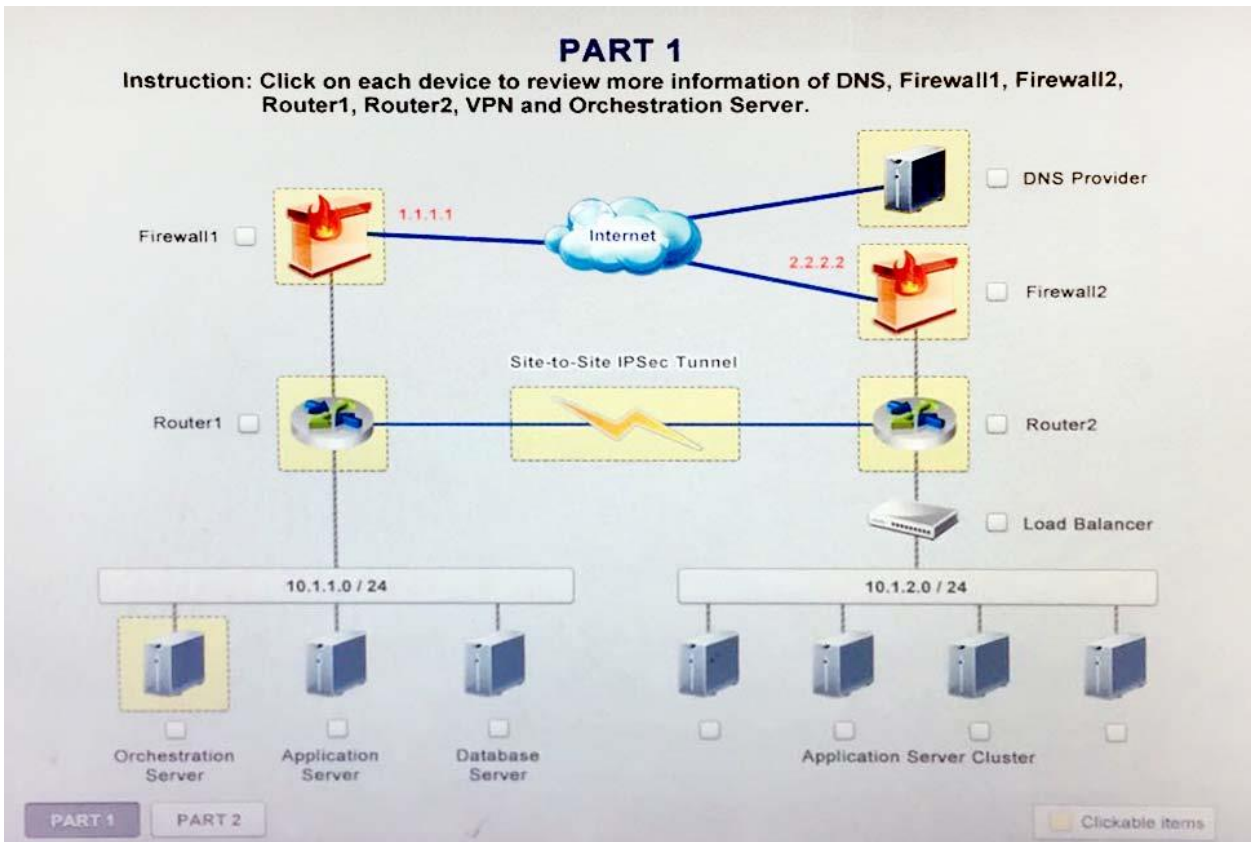2. Identify the problematic device(s).
:

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

Firewall1

Firewall1 Configuration

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

Firewall2

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

1.1.1.1

Internet

Firewall2

Router1 [−] [×]

Router1 Configuration

Public IP: 1.1.1.1

Internal IP: 10.1.1.1/24

Router1

Site-to-Site VPN Configuration

Address Space: 10.1.1.0/24

Router2

Subnet: 255.255.255.0

PSK: Cloud001

Load Balancer

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

Orchestration Server

Application Server

Database Server

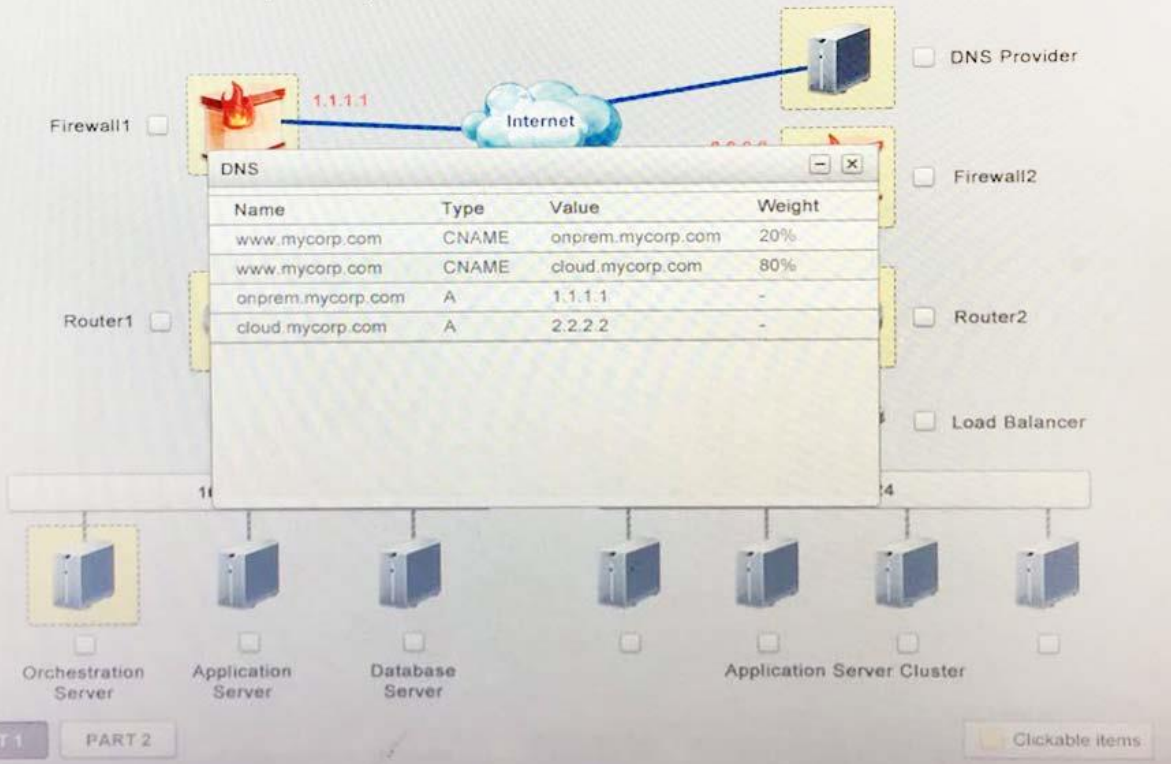Application Server Cluster

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

DNS [−] [×]

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

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 [−] [×]

Firewall2 Configuration

Source	Destination	Port
any	2.2.2.2	80.443
10.1.2.0/24	any	any
any	any	deny

Firewall2

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

Site-to-Site VPN Configuration
Address Space: 10.1.1.0/24
Subnet: 255.255.255.0
PSK: Cloud002
IKE: SHA1/AES256/DH2/SA Lifetime 28800

Firewall2

Router1   Router2

Load Balancer

Orchestration Server   Application Server   Database Server   Application Server Cluster

PART 1   PART 2
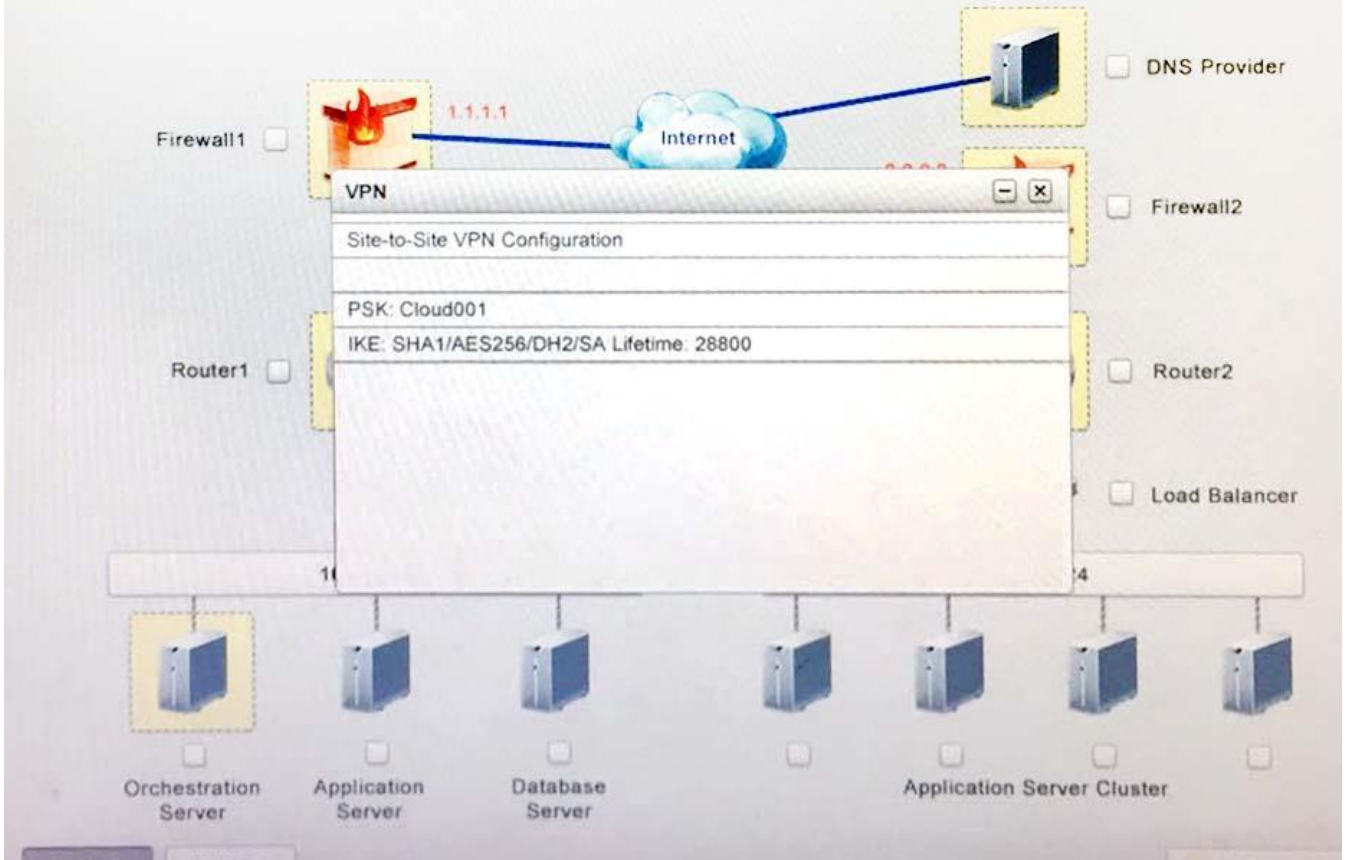
PART 1

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

DNS Provider

Firewall1

1.1.1.1

Internet

VPN [-] [×]

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

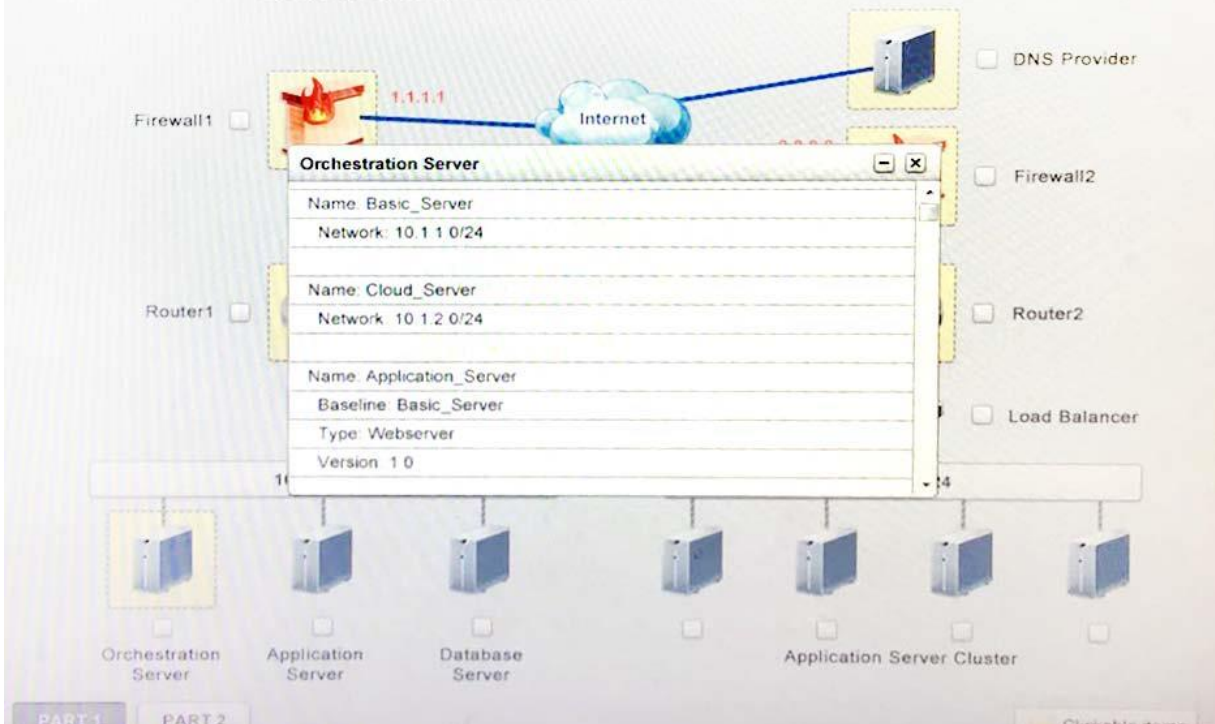# PART 1

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.

Firewall1

1.1.1.1

Internet

DNS Provider

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

Router1

Router2

Load Balancer

Orchestration
Server

Application
Server

Database
Server

Application Server Cluster

PART 1   PART 2

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

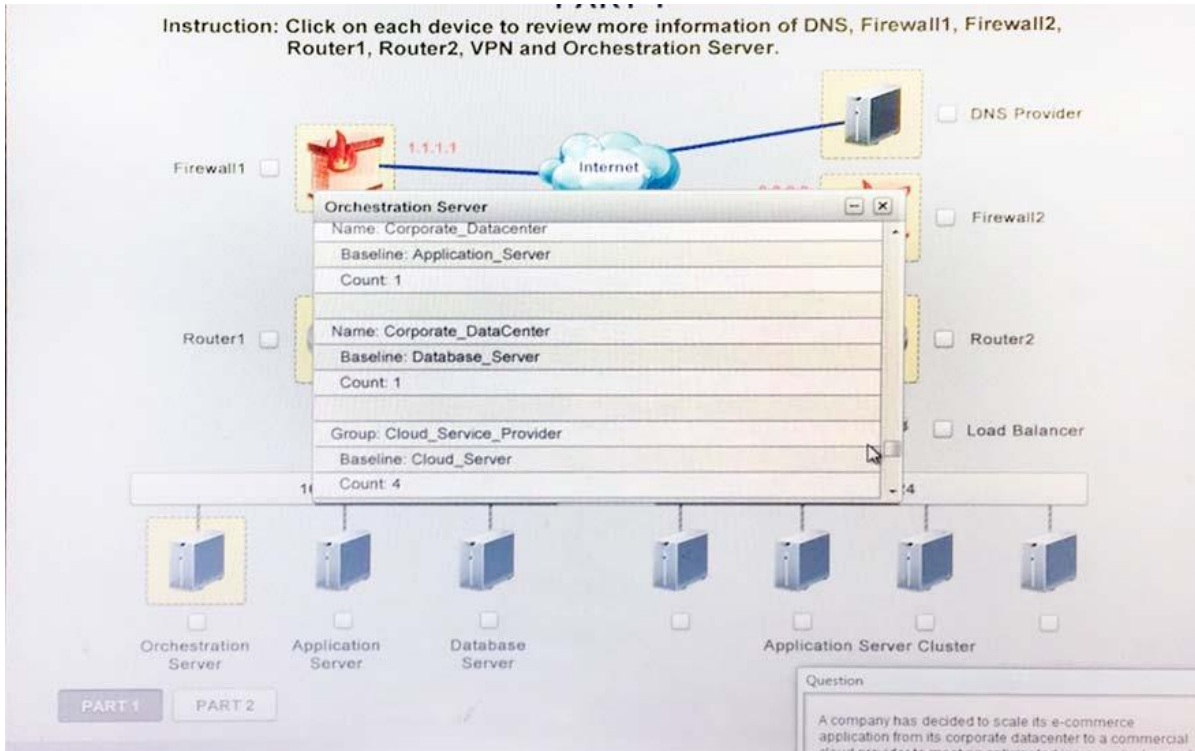Application
Server

Database
Server

Application Server Cluster

PART 1   PART 2

Correct Answer: See the solution below.

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: Corporate_Datacenter
Baseline: Application_Server
Count: 1

Firewall2

Router1
Name: Corporate_DataCenter
Baseline: Database_Server
Count: 1

Router2

Group: Cloud_Service_Provider
Baseline: Cloud_Server
Count: 4

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
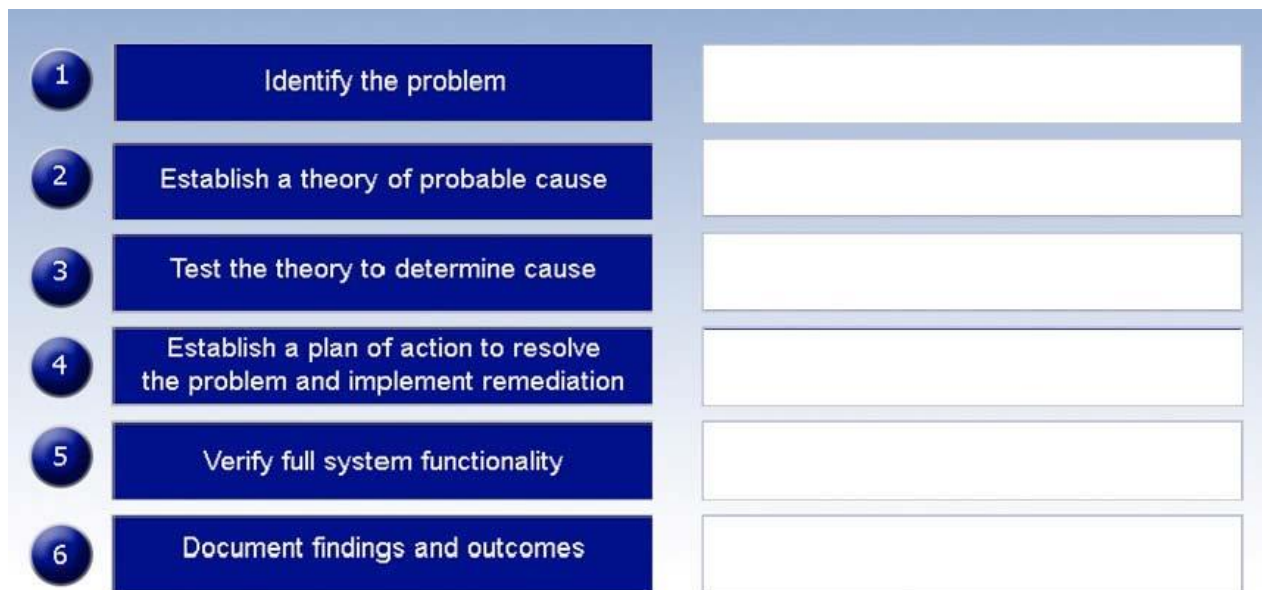
Question #3

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.
Select and Place:

1

2

3

4

5

6

Establish a plan of action to resolve the problem and implement remediation

Establish a theory of probable cause

Document findings and outcomes

Identify the problem

Test the theory to determine cause

Verify full system functionality

Correct
Answer:

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

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

Correct Answer: B
Reference -
https://www.acronis.com/en-us/blog/posts/tips-tricks-better-business-backup-and-recovery-world-backup-day