Vendor: Check Point

Exam Code: 156-561

Exam Name: Check Point Certified Cloud Specialist – R81.20 (CCCS)

Version: DEMO

QUESTION 1
Which solution allows administrators to manage, control, and monitor access to important resources in your Azure environment?

A. Azure Open Directory Service
B. Azure Active Directory
C. iPlanet Directory Service
D. Azure Directory Federation Service

Answer: B
Explanation:
Azure Active Directory (Azure AD) is the solution that allows administrators to manage, control, and monitor access to important resources in an Azure environment. It provides identity and access management capabilities, enabling secure access to cloud applications and resources, and helps in managing users, groups, and permissions across various services within Azure.

QUESTION 2
Responsibility for securing Software Defined Data Centers resides with which of the following?

A. Cloud Service Consumers only
B. Cloud Service Providers and Consumers
C. Cloud Service Providers only
D. Individual Corporate Users

Answer: B
Explanation:
In a Software Defined Data Center (SDDC), the responsibility for security is shared between the Cloud Service Provider (CSP) and the Cloud Service Consumer. The CSP is responsible for securing the underlying physical infrastructure and providing secure tools for management, while the consumer is responsible for securing their own data, applications, and configurations within the SDDC. This shared responsibility model ensures both parties play a role in maintaining the security of the cloud environment.

QUESTION 3
Which is not a limitation of a Security Gateway Cluster deployment?

A. Virtual Router Redundancy Protocol (VRRP)
B. Clusters must include a maximum of two members
C. ClusterXL load sharing
D. Both cluster members must reside in different regions and locations for redundancy

Answer: D
Explanation:
This is not a limitation of a Security Gateway Cluster deployment. In fact, Security Gateway clusters can be deployed within the same region and still provide high availability and redundancy.

QUESTION 4
What is true about Terraform?

A. It utilizes Playbooks written in JSON

B. It uses ACL Hiyashi scripting system
C. It utilizes Playbooks written in YAML
D. It was created by Red Hat

Answer: C
Explanation:
Terraform is an Infrastructure as Code (IaC) tool used to define and provision infrastructure in a declarative manner. Terraform configurations are written in HCL (HashiCorp Configuration Language), but it also supports YAML for certain integrations. Playbooks, however, are typically associated with Ansible, not Terraform, but Terraform can still use YAML-based configurations in some cases.

QUESTION 5
What makes up a Hybrid Data Center Deployment?

A. This is a deployment in which data can be stored in the AWS's BLOB storage and the corresponding Meta data in the file server located in the organization's on-premises data center.
B. Some components of the data center reside in an organization's on-premises data center, and some are housed by a Cloud Service Provider in their Cloud-based data center.
C. This is a single-cloud environment in which some resources need the authorization via the local Active Directory Domain Controller and some other resources via the AWS Active Directory.
D. This is a multi-cloud environment in which some workloads are run in an Amazon AWS Cloud and others in a cloud of another CSP, such as Microsoft Azure or Google Cloud.

Answer: B
Explanation:
A Hybrid Data Center Deployment involves a combination of on-premises data center infrastructure and cloud-based resources from a Cloud Service Provider (CSP). This model allows organizations to keep certain resources on-premises while utilizing the scalability and flexibility of the cloud for other workloads, offering a hybrid approach to infrastructure management.

QUESTION 6
What is one of the purposes of the South Hub in a Hybrid Datacenter deployment?

A. To inspect traffic arriving into the environment from the internet
B. To secure traffic between the spoke networks and the on-premises data center
C. To ease email communication with the Cloud Service Provider
D. To secure Remote Access connections to the environment

Answer: B
Explanation:
In a Hybrid Data Center deployment, the South Hub is responsible for securing traffic between cloud-based spoke networks (such as AWS VPCs or Azure subnets) and the on-premises data center. It ensures secure communication, typically through mechanisms like VPNs, to connect cloud resources with on-premises infrastructure, maintaining security and control over the traffic flow.

QUESTION 7
In the Cloud Security Blueprint, the Spokes...

A. handle non-transitive traffic between peered networks
B. handle inbound and customer-facing traffic
C. House the cloud Workloads
D. handle internal spoke to spoke traffic, Spoke to Internet (Egress) traffic, and cloud to on-premises traffic

Answer: C
Explanation:
In the Cloud Security Blueprint, Spokes are responsible for housing the cloud workloads. They are isolated segments within the cloud network where specific applications, services, or workloads are deployed. The spokes are typically connected to other network components like hubs, which manage traffic and ensure security, but the primary role of the spokes is to host the cloud resources.

QUESTION 8
What methods might a customer use to connect their on-premise datacenter to the cloud datacenter?

A. Through a hub and spoke
B. Site to Site VPN or Azure Express Route
C. Azure Active Directory
D. Azure Arc

Answer: B
Explanation:
To connect an on-premise data center to a cloud data center, a customer typically uses Site-to-Site VPN or Azure ExpressRoute.
Site-to-Site VPN provides a secure, encrypted connection over the internet between the on-premises network and the cloud network.
Azure ExpressRoute offers a private, dedicated connection to Azure from the on-premises data center, providing higher reliability, speed, and security compared to a standard VPN.

Both methods are commonly used for hybrid cloud connectivity, ensuring secure communication between on-premises and cloud environments.

QUESTION 9
In the Cloud Security Blueprint, the North Hub handles...

A. House the cloud Workloads
B. Non-transitive traffic between peered networks
C. Internal spoke to spoke traffic, Spoke to Internet (Egress) traffic, and cloud to on-premises traffic
D. Inbound and customer-facing traffic

Answer: D
Explanation:
In the Cloud Security Blueprint, the North Hub is responsible for handling inbound and customer-facing traffic. This includes managing and securing the traffic coming from external sources (like the internet) into the cloud environment. The North Hub typically acts as a centralized point for managing security policies for such external communications.

QUESTION 10

The Cloud Security Blueprint consists of the following elements:

A. Blue zone, Red zone and Yellow Zone
B. Standalone and Distributed Gateways
C. North Hub, South Hub and Spokes
D. Site-to-Site and Remote Access VPNs

Answer: C
Explanation:
The Cloud Security Blueprint consists of key components like the North Hub, South Hub, and Spokes. These elements define how traffic flows within the cloud network, where:
North Hub handles inbound and customer-facing traffic.
South Hub secures traffic between spoke networks and the on-premises data center.
Spokes house the cloud workloads and are connected to other network components.

This architecture provides a secure, organized way to manage traffic and resources in a cloud environment.

QUESTION 11
According to secure Public Cloud guidelines, CloudGuard Security Gateways should reside where?

A. In a subnet with other cloud resources within the network.
B. In a hub subnet along with other virtual machines in the network.
C. In a zone that contains multiple subnets.
D. In a hub subnet that does not contain any other virtual machines.

Answer: D
Explanation:
According to secure Public Cloud guidelines, CloudGuard Security Gateways should reside in a hub subnet that does not contain any other virtual machines. This setup ensures that the security gateway can act as a central point to inspect and secure traffic between different network segments (such as between spokes, on-premises networks, and the internet) without interfering with the workloads hosted in other subnets or zones.

QUESTION 12
What is the Cloud Management Extension used for?

A. Importing objects from the cloud
B. Deploying hotfixes
C. Managing autoscaling gateways
D. Cloud logging

Answer: C
Explanation:
The Cloud Management Extension (CME) is used for managing autoscaling gateways in cloud environments. It helps automate the deployment, scaling, and management of security gateways in cloud environments, ensuring they scale dynamically based on the cloud resources and workload demands. CME integrates with cloud environments like AWS, Azure, and others to optimize security and network management.

QUESTION 13
In Azure with CloudGuard Gateways deployed as an HA cluster, how does cluster sync and failover work?

A. Customer has to build an operational model to manually invoke failover for CloudGuard Gateway HA cluster running in Azure
B. In cloud, this is all via API. The CloudGuard Gateway cluster failover is performed over API calls to Azure and uses Azure Active Directory Service account to change IP and routing to the new active gateway
C. Multicast or broadcast communicate state synchronization and health checks across cluster members
D. Cluster sync and failover are not possible for CloudGuard Gateway HA cluster in Azure

Answer: B
Explanation:
In Azure, CloudGuard Gateway HA cluster failover and synchronization are handled via API calls. The API interfaces with Azure services, utilizing the Azure Active Directory service account to facilitate the failover process by changing the IP and routing to the new active gateway. This approach automates the failover, ensuring minimal downtime and efficient cluster management.

QUESTION 14
What mechanism is used in the Cloud during a ClusterXL fail-over scenario?

A. The Router Discovery protocol will be used to propagate the new route after a failover scenario.
B. Cloud clusters perform failovers by making API calls to the CSP.
C. The Neighbor Discovery protocol will be used to propagate the new cluster node to be forwarded the packets to.
D. The Gratuitous ARP mechanism will be used to change the MAC address entry in the ARP cache of the router.

Answer: C
Explanation:
In cloud environments, particularly when using IPv6, Neighbor Discovery Protocol (NDP) is used during a ClusterXL failover scenario to propagate the new cluster node. NDP helps in updating the network to reflect the new node and ensures that traffic is correctly forwarded to the active node in the cluster. Unlike traditional on-premises environments that use Gratuitous ARP (GARP), cloud environments typically rely on NDP for handling failovers in IPv6 networks.

QUESTION 15
During a cluster failover event in Azure, the standby will do which of the following?

A. Sends health probe packets
B. Sends out a GARP
C. Tries to ping the other member
D. Associate the cluster public IP with its external interface

Answer: D
Explanation:
During a cluster failover event in Azure, the standby node will associate the cluster public IP with its external interface. This action ensures that the standby node takes over the active role, allowing it to handle incoming traffic by assigning the public IP that was previously associated with the active node, maintaining seamless access and connectivity.

QUESTION 16
The Auto Scaling solution is an example of which of the following?

A. Horizontal scaling
B. Amazon Elastic Kubernetes Service
C. Vertical scaling
D. Amazon Elastic Container Service

Answer: A
Explanation:
Auto Scaling in cloud environments, such as AWS, is an example of horizontal scaling. Horizontal scaling involves adding or removing instances (virtual machines or containers) to increase or decrease capacity based on demand, rather than increasing the resources (like CPU or memory) of a single instance, which is known as vertical scaling. Auto Scaling automatically adjusts the number of instances in response to changing traffic or load, making it a form of horizontal scaling.

QUESTION 17
In AWS with CloudGuard Gateways deployed as an HA cluster, how does cluster sync and failover work?

A. Multicast or broadcast communicate state synchronization and health checks across cluster members
B. Customer has to build an operational model to manually invoke failover for CloudGuard Gateway HA cluster running in AWS
C. In cloud, this is all via API. The CloudGuard Gateway cluster failover is performed over API calls to AWS and uses IAM role to change IP and routing to the new active gateway
D. Cluster sync and failover are not possible for CloudGuard Gateway HA cluster in AWS

Answer: C
Explanation:
In AWS, CloudGuard Gateway HA cluster failover and synchronization are managed through API calls. When a failover occurs, the cluster failover process is automated by using AWS APIs and IAM roles. These APIs allow the system to dynamically change the IP address and routing to the new active gateway without manual intervention, ensuring high availability and seamless failover in the cloud environment.

QUESTION 18
The Cluster Control Protocol uses which Protocol/Port Combination?

A. UDP 256
B. TCP 8116
C. UDP 8116
D. TCP 18197

Answer: C
Explanation:
The Cluster Control Protocol (CCP) uses UDP port 8116 for communication between the members of a cluster. This protocol is responsible for synchronization and state sharing among the cluster members, ensuring that the cluster operates cohesively during failover and load balancing scenarios.

QUESTION 19
What is a required Software Blade which has to be activated along with a CloudGuard Controller?

A. The Identity Awareness Software Blade
B. The IPSec VPN Software Blade
C. The Mobile Access Software Blade
D. The User Directory Software Blade

Answer: A
Explanation:
When deploying a CloudGuard Controller, the Identity Awareness Software Blade is typically required to be activated. This blade enables the controller to integrate with identity systems (such as Active Directory) and apply security policies based on user identities, providing context for traffic inspection and security enforcement in cloud environments.

QUESTION 20
The ARM templates are defined in this format

A. Extensible Markup Language (XML)
B. JavaScript Object Notation (JSON)
C. Python
D. YAML Ain't Markup Language (YAML)

Answer: B
Explanation:
Azure Resource Manager (ARM) templates are defined in JSON (JavaScript Object Notation) format. These templates describe the resources you want to deploy in your Azure environment, allowing you to define, configure, and provision Azure infrastructure as code. JSON is a lightweight, easy-to-read format commonly used for such configurations.

QUESTION 21
What file format is used for Azure templates?

A. JSON
B. YAML
C. SGML
D. Python

Answer: A
Explanation:
Azure templates, specifically Azure Resource Manager (ARM) templates, are defined in JSON (JavaScript Object Notation) format. This format is used to describe the resources, configurations, and deployments in Azure, enabling infrastructure as code for consistent and automated resource provisioning.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**