Question 1

Fill in the blanks: Default port numbers for an LDAP server is _____ for standard connections and SSL connections.

Options:

A- 443,389

B- 636; 8080

C- 290; 3389

D- 389; 636

Answer:

D

Explanation:

LDAP (Lightweight Directory Access Protocol) operates over different ports, with each serving a specific purpose. Port389is the default port for unsecured LDAP connections or LDAP with StartTLS, which upgrades the connection to use TLS (Transport Layer Security) for

LDAP Ports Explained: Configuring Standard, StartTLS, and LDAPS Connections

Red Hat Directory Server documentation on changing LDAP and LDAPS port numbers

Oracle documentation on Directory Server and Directory Proxy Server LDAP and LDAPS Port Numbers

ServerFault discussion on LDAP server authentication ports

Question 2

Question Type: **MultipleChoice**

Fill in the blank: An identity server uses a _____ to trust a Terminal Server Identity Agent.

Options:

A- Shared secret

B- One-time password

C- Certificate

D- Token

Answer:

A

Explanation:

When configuring Terminal Servers with Identity Awareness, you must configure the same password as a shared secret in both the Terminal Servers Identity Agent on the application server that hosts the Terminal/Citrix services and on the Identity Awareness Gateway.This shared secret enables secure communication and allows the Security Gateway to trust the application server with the Terminal Servers functionality1.

Check Point Software - Configuring Terminal Servers

Check Point Identity Awareness Clients Admin Guide

Check Point Troubleshooting Expert - R81 (CCTE) Reference Materials

Check Point Certified Troubleshooting Expert R81.20 - CCTE

Check Point CCTE Certification Sample Questions and Practice Exam

Question 3

Identity Awareness allows easy configuration for network access and auditing based on what three items?

Options:

A- Client machine IP address.

B- Network location, the identity of a user and the identity of a machine

C- Log server IP address.

D- Gateway proxy IP address.

Answer:

B

Explanation:

Identity Awareness maps users and computer identities, enabling enforcement of Access Control policy rules and auditing data based on identity.It is an easy-to-deploy and scalable solution that works for both Active Directory and non-Active Directory based networks,

including employees and guest users1.By considering network location, user identity, and machine identity, organizations can control access between different segments in the network using an identity-based policy2.

Question 4

Question Type: **MultipleChoice**

Which of the following is NOT a method used by Identity Awareness for acquiring identity?

Options:

A- Remote Access

B- Active Directory Query

C- Cloud IdP (Identity Provider)

D- RADIUS

Answer:

A

Explanation:

Identity Awareness uses various methods to acquire identity information. These methods include:

Active Directory Query: Identity Awareness queries Active Directory servers to retrieve user and group information.

Cloud IdP (Identity Provider): Identity Awareness integrates with cloud identity providers such as Microsoft Azure AD, Okta, and Google Workspace.

RADIUS: Identity Awareness can use RADIUS servers to authenticate users.

However, Remote Access is not a method used by Identity Awareness for acquiring identity. Remote Access typically refers to VPN connections, and while Identity Awareness can be used in conjunction with VPNs, it does not directly acquire identity information from remote access connections.

Check Point Troubleshooting Expert - R81 (CCTE) Reference Materials guides and documents.

Check Point Certified Troubleshooting Expert R81.20 - CCTE

Check Point CCTE Certification Sample Questions and Practice Exam

Question 5

The back-end database for Check Point Management uses:

Options:

A- PostgreSQL

B- MongoDB

C- MySQL

D- DBMS

Answer:

B

Explanation:

Check Point Management uses MongoDB as its back-end database. MongoDB is a NoSQL database that offers high performance, high availability, and easy scalability, which are essential for managing the complex and dynamic nature of network security configurations and logs.

Question 6

Fill in the blank RADIUS protocol uses_____to communicate with the gateway

Options:

A- TDP

B- CCP

C- HTTP

D- UDP

Answer:

D

Question 7

identity Awareness allows easy configuration for network access, and auditing based on what three items?

Options:

A- Client machine IP address

B- Network location the identity of a user and the identity of a machine

C- Log server IP address

D- Gateway proxy IP address

Answer:

B

Question 8

Which Identity Source(s) should be selected in Identity Awareness Tot when there is a requirement for a higher level of security for sensitive servers?

Options:

A- Endpoint identity Agent and Browser Based Authentication

B- AD Query

C- Terminal Servers Endpoint Identity Agent

D- RADIUS and Account Logon

Answer:

A