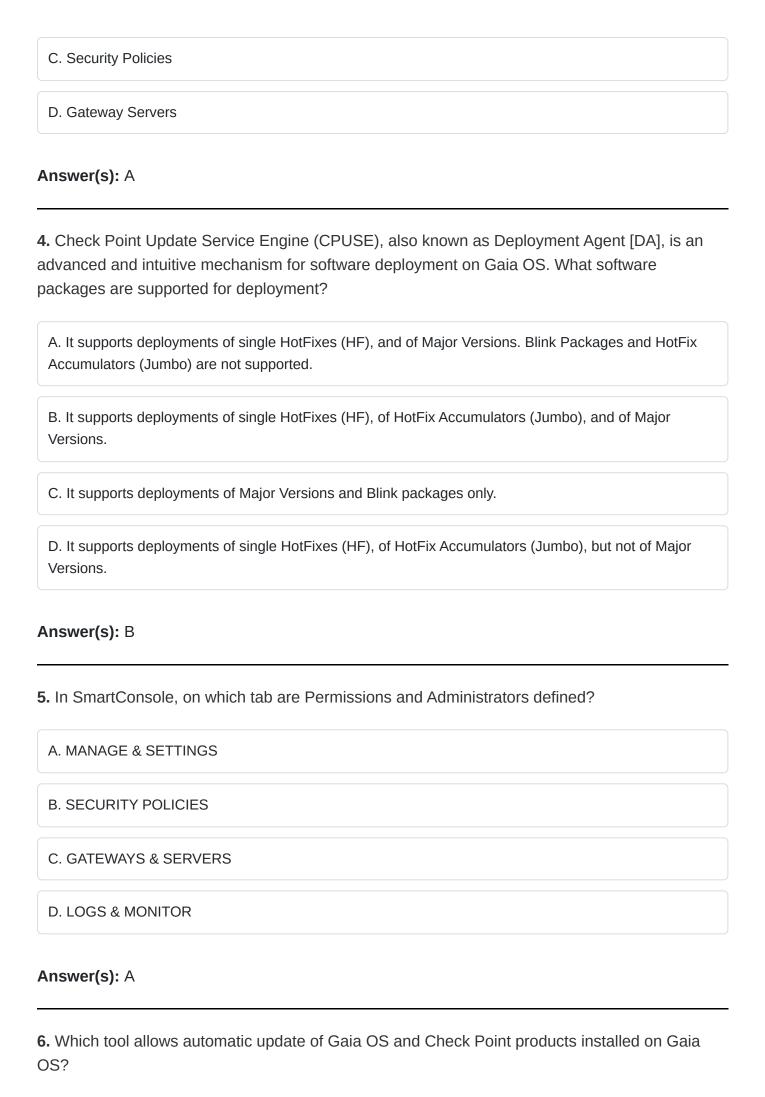# Check Point Certified Security Administrator – R81.20 (CCSA)

1. Which default Gaia user has full read/write access?

A. superuser

B. monitor

C. altuser

D. admin

Answer(s): D

---

2. Which icon in the WebUI indicates that read/write access is enabled?

A. Eyeglasses

B. Pencil

C. Padlock

D. Book

Answer(s): B

---

3. Which SmartConsole tab is used to monitor network and security performance?

A. Logs Monitor

B. Manage Settings

C. Security Policies

D. Gateway Servers

Answer(s): A

---

4. Check Point Update Service Engine (CPUSE), also known as Deployment Agent [DA], is an advanced and intuitive mechanism for software deployment on Gaia OS. What software packages are supported for deployment?

A. It supports deployments of single HotFixes (HF), and of Major Versions. Blink Packages and HotFix Accumulators (Jumbo) are not supported.

B. It supports deployments of single HotFixes (HF), of HotFix Accumulators (Jumbo), and of Major Versions.

C. It supports deployments of Major Versions and Blink packages only.

D. It supports deployments of single HotFixes (HF), of HotFix Accumulators (Jumbo), but not of Major Versions.

Answer(s): B

---

5. In SmartConsole, on which tab are Permissions and Administrators defined?

A. MANAGE & SETTINGS

B. SECURITY POLICIES

C. GATEWAYS & SERVERS

D. LOGS & MONITOR

Answer(s): A

---

6. Which tool allows automatic update of Gaia OS and Check Point products installed on Gaia OS?

A. CPDAS - Check Point Deployment Agent Service

B. CPUSE - Check Point Upgrade Service Engine

C. CPASE - Check Point Automatic Service Engine

D. CPAUE - Check Point Automatic Update Engine

Answer(s): B

---

7. In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server?

A. Verify and compile Security Policies.

B. Display policies and logs on the administrator's workstation.

C. Store firewall logs to hard drive storage.

D. Manage the object database.

Answer(s): B

---

8. True or False: More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time.

A. True, every administrator works on a different database that is independent of the other administrators

B. False, only one administrator can login with write permission

C. True, every administrator works in a session that is independent of the other administrators

D. False, this feature has to be enabled in the Global Properties

Answer(s): C

---

9. What Check Point tool is used to automatically update Check Point products for the Gaia OS?

A. Check Point Update Engine

B. Check Point Upgrade Installation Service

C. Check Point Upgrade Service Engine (CPUSE)

D. Check Point INSPECT Engine

Answer(s): C

---

10. If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer.

A. Delete older versions of database.

B. Publish or discard the session.

C. Revert the session.

D. Save and install the Policy.

Answer(s): B

---

11. What are the two deployment options available for a security gateway?

A. Bridge and Switch

B. Local and Remote

C. Cloud and Router

D. Standalone and Distributed

Answer(s): D

12. One of major features in SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

A. AdminB sees a pencil icon next the rule that AdminB is currently editing.

B. AdminA, AdminB and AdminC are editing three different rules at the same time.

C. AdminA and AdminB are editing the same rule at the same time.

D. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.

Answer(s): C

---

13. Which one of the following is the preferred licensing model? Select the BEST answer.

A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.

B. Local licensing because it ties the package license to the MAC-address of the gateway management interface and has no Security Management Server dependency.

C. Central licensing because it ties the package license to the IP-address of the Security Management Server and has no dependency on the gateway.

D. Central licensing because it ties the package license to the MAC-address of the Security Management Server's Mgmt-interface and has no dependency on the gateway.

Answer(s): C

---

14. A Check Point Software license consists of two components, the Software Blade and the Software Container. There are _____ types of Software Containers: _____.

A. Two; Security Management and Endpoint Security

B. Three; Security Management, Security Gateway, and Endpoint Security

C. Three; Security Gateway, Endpoint Security, and Gateway Management

D. Two; Endpoint Security and Security Gateway

Answer(s): C

---

15. Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

A. Formal

B. Central

C. Local

D. Corporate

Answer(s): C

---

16. Tom has connected to the Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made?

A. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.

B. Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.

C. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

D. Tom's changes will be lost since he lost connectivity and he will have to start again.

Answer(s): C

---

17. In which deployment is the security management server and Security Gateway installed on the same appliance?

A. Switch

B. Standalone

C. Distributed

D. Remote

Answer(s): B

---

18. Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?

A. Data Awareness

B. Threat Emulation

C. Application Control

D. Identity Awareness

Answer(s): D

---

19. DLP and Mobile Access Policy are examples of what type of Policy?

A. Shared Policies

B. Unified Policies

C. Inspection Policies

D. Standard Policies

Answer(s): A

---

20. What is the default shell of Gaia CLI?

A. Read-only

B. Expert

C. Clish

D. Bash

Answer(s): C