220-1101 Q&As

CompTIA A+ Certification Exam: Core 1

Pass CompTIA 220-1101 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/220-1101.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following components enables the input on a mobile device\\'s touch screen?

A. OLED

B. Digitizer

C. Inverter

D. CMOS sensor

Correct Answer: B

The digitizer is the component that enables input on a mobile device\\'s touch screen. It is a transparent layer that sits over the screen and detects the location of touch inputs. OLED (Organic Light Emitting Diode) is a type of display technology. Inverter is a component used in older LCD displays to provide power to the backlight. CMOS (Complementary Metal-Oxide-Semiconductor) sensor is a type of image sensor used in digital cameras and smartphones to capture images. References: CompTIA A+ Certification Exam: Core 1 - Page 177

QUESTION 2

A university student was able to boot from a live Linux CD on a computer in a shared space on campus. Which of the following will BEST prevent this type of action from occurring in the future?

A. Require TPM security features.

B. Set a boot password.

C. Disable all media options.

D. Enable secure boot.

Correct Answer: D

Enabling secure boot will verify the digital signature of the bootloader and operating system, ensuring that the system only boots from trusted and authorised sources. This can prevent booting from an unauthorised live CD or other external media. The best way to prevent booting from a live Linux CD on a computer in a shared space on campus is to enable secure boot. Secure boot is a feature that ensures that the system only runs software that is signed by an authorized party. This means that the system will not boot from any unauthorized media, including live Linux CDs. Secure Boot is a feature that ensures that the system only runs software that is signed by an authorized party. This means that the system will not boot from any unauthorized media, including live Linux CDs. Secure Boot is an important security feature designed to prevent malicious software from loading when your PC starts up (boots)1. Booting from a live Linux CD is a process that allows you to run a Linux operating system from a CD or DVD without installing it on your hard drive. This can be useful for testing or troubleshooting purposes. To boot from a live Linux CD, you need to insert the CD or DVD into your computer\\'s CD/DVD drive and restart your computer. Most systems are set up to automatically boot from the CD/DVD drive, but if your system is not set up this way, you may need to change a system setting to boot from a Linux CD/DVD23.

QUESTION 3

A company would like to take advantage of the cost savings of cloud computing by only paying for the resources used. Which of the following will BEST address this need?

A. Shared resources

B. Rapid elasticity

C. Metered utilization

D. High availability

Correct Answer: C

Metered utilization is a cloud feature that allows cloud providers to charge customers based on their actual consumption of resources, such as CPU time, storage space, bandwidth, or transactions.This enables customers to pay only for the

resources they use, rather than a fixed or flat rate, which can reduce costs and increase efficiency. Metered utilization can also provide more transparency and accountability for both cloud providers and customers, as they can track and

monitor their resource usage and billing.

Reference: https://partners.comptia.org/docs/default-source/resources/a-core-1-content-guide (page 97)

QUESTION 4

Which of the following network devices operates as a bridge function?

A. Hub

B. Wireless access point

C. Transceiver

D. Media converter

Correct Answer: D

A media converter is a network device that operates as a bridge function, which means it connects two different types of network media, such as copper and fiber optic cables, and converts signals between them. This allows network devices

that use different media types to communicate with each other over long distances or in different environments, without requiring major changes or upgrades to the existing network infrastructure.

Reference: https://www.comptia.org/training/books/a-core-1-220-1101-study- guide (page 73)

QUESTION 5

A technician is attempting to connect the wired LANs at two nearby buildings by installing a wireless point-to-point connection. Which of the following should the technician consider?

A. NFC protocol data rate

B. RFID frequency range

C. Bluetooth version compatibility

D. Allowable limits for transmit power

Correct Answer: D

When installing a wireless point-to-point connection between two buildings, the technician should consider the allowable limits for transmit power, which vary depending on the country or region. Exceeding these limits could interfere with other wireless devices or violate regulations. NFC protocol data rate, RFID frequency range, and Bluetooth version compatibility are not relevant for a wireless point-to-point connection.