N10-008^{Q&As}

N10-008^{Q&As}

CompTIA Network+

Pass CompTIA N10-008 Exam with 100% Guarantee

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

https://www.passapply.com/n10-008.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

A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:

1.

Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down

2.

Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down

Which of the following describes the reason why the events are not being received?

A. The network device is not configured to log that level to the syslog server

B. The network device was down and could not send the event

C. The syslog server is not compatible with the network device

D. The syslog server did not have the correct MIB loaded to receive the message

Correct Answer: A

The syslog severity levels are 0 (Emergency), 1 (Alert), 2 (Critical), 3 (Error), 4 (Warning), 5 (Notice/Notification), 6 (Information), and 7 (Debugging). An easy mnemonic to memorize this is "Emus Are Cute Even When In Disguise." Because the device is set to send CRITICAL events, it will send only events that have a severity level of 2 and below. Thus, you have to configure the device to send events at severity level 5 or higher.

QUESTION 2

A help desk supervisor discovers the following ticket excerpt while reviewing notes in a customer\\'s account:

1.

Received report that customer was unable to use the scanner to read barcodes, the internet no longer worked, and the monitor was fuzzy. Arrived on site and began troubleshooting.

2.

Confirmed monitor issue. Replaced VGA cable.

3.

Confirmed scanner failure. Scanner USB cable was unattached. Reattached cable.

4.

Confirmed internet issue. Duplicated on test laptop. Escalated to ISP.

Which of the following BEST describes what the technician was doing?

A. The technician was questioning the obvious.

B. The technician was implementing preventative measures.

C. The technician was approaching multiple problems individually.

D. The technician was determining if anything had changed.

Correct Answer: C

QUESTION 3

Which of the following, in addition to a password, can be asked of a user for MFA?

A. PIN

B. Favorite color

C. Hard token

D. Mother\\'s maiden name

Correct Answer: A

MFA stands for Multi-Factor Authentication, which is a method of verifying the identity of a user by requiring two or more pieces of evidence that belong to different categories:

something the user knows, something the user has, or something the user is. A password is something the user knows, and it is usually combined with another factor such as a PIN (Personal Identification Number) or a hard token (a physical

device that generates a one- time code) that the user has. A favorite color or a mother\\'s maiden name are not suitable for MFA, as they are also something the user knows and can be easily guessed or compromised.

QUESTION 4

Users report that the network is slower than usual when accessing on-premises email. Which of the following should a network technician do to confirm the issue?

A. Review the logging levels of network devices.

B. Check the audit logs to see if users are accessing email

C. Compare the network baselines to the current network status.

D. Verify that users who are trying to access email have LDAP accounts

Correct Answer: C

QUESTION 5

A network contains 25 access points. Which of the following devices would be best to change configurations on all the devices remotely?

A. WLAN controller

B. Load balancer

C. Bridge

D. Layer 3 switch

Correct Answer: A

A WLAN controller is a device that can centrally manage and configure multiple access points in a wireless network. A WLAN controller can change settings on all the devices remotely, such as SSIDs, security policies, firmware updates, and channel assignments. A WLAN controller can also monitor the performance and status of the access points and provide load balancing and fault tolerance