Exam Report: 15.7.4 Practice Questions

Date: 12/7/2019 10:08:30 pm
Time Spent: 13:13

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 75%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You are the network administrator for a growing business. When you were hired, the organization was small, and only a single switch and router were required to support your users. During this time, you monitored log messages from your router and switch directly from each device's console.

The organization has grown considerably in recent months. Now you manage eight individual switches and three routers. It's becoming more and more difficult to monitor these devices and stay on top of issues in a timely manner.

What should you do?

- Use syslog to implement centralized logging.
- Use a remote access utility such as SSH to access router and switch consoles remotely.
- Consolidate network resources down to one or two switches.
- Hire additional resources to help monitor and manage your network infrastructure.

Explanation

In this scenario, a cost-effective option would be to implement centralized logging using syslog. By default, routers and switches send all log messages for all severity levels directly to the console. If a network contains a small number of devices, this default configuration is usually manageable. However, on a growing network, it quickly becomes impractical to visit each device to view log messages. Instead, you can configure your network devices to redirect logging to a syslog server somewhere in the network. By doing this, all log messages from all devices can be consolidated and viewed from a single location.

Reducing the number of switches on a growing network is generally not advisable. Using a remote access utility can help alleviate the issue to an extent. However, you still have to manually connect to and monitor each individual system. If the network continues to grow, this option will quickly become unviable. It's not necessary to hire additional administrators in this scenario.

References

LabSim for Network Pro, Section 15.7.
[netpro18v5_all_questions_en.exm MCS5]

Question 2: Correct

Which of the following is a standard for sending log messages to a central logging server?

- OVAL
- Syslog
- Nmap
- LC4

Explanation

Syslog is a protocol that defines how log messages are sent from one device to a logging server on an IP network. The sending device sends a small text message to the syslog receiver (the logging server).
The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system. LC4 (previously called LOphtcrack) is a password cracking tool. Nmap is a network mapping tool that performs ping and port scans.

References

LabSim for Network Pro, Section 15.7.
[netpro18v5_all_questions_en.exm SP08_4-6 3]

Question 3: Incorrect

Consider the following output generated by the **show interface fa0/0** command generated on a router:

FastEthernet0/0 is up, line protocol is up
[...]
Auto-duplex, 100Mb/s, 100BaseTX/FX
[...]
Input queue: 0/75/1771/0 (size/max/drops/flushes); Total output drops: 0
[...]
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
15387 packets input, 1736263 bytes, 0 no buffer
Received 15241 broadcasts, 0 runts, 0 giants
0 input errors, 1 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast
0 input packets with dribble condition detected
607 packets output, 6141 bytes, 0 underruns
4 output errors, 10 collisions, 3 interface resets, 0 restarts
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

Which of the following statements are true about the fa0/0 interface? (Select three.)

- [x] ~~The interface is running in half-duplex mode.~~
- [x] Several collisions have occurred.
- [x] The interface is dropping incoming packets.
- [ ] There have been no interface resets.
- [ ] One cyclic redundancy check error has occurred.
- [ ] No input **or** output errors have occurred.

Explanation

The **show interface** command can help you identify problems that have occurred on an interface.
Consider the following output generated by the **show interface fa0/0** command generated on a router:

FastEthernet0/0 is up, line protocol is up
[...]

Based on the output, the following information can be identified:

- 1771 packets have been dropped.
- Auto-duplex mode is selected.
- One CRC error has occurred.
- Three interface resets have occurred.
- Zero input errors have occurred, but there have been four output errors.
- 10 collisions have occurred.

References

LabSim for Network Pro, Section 15.7.
[netpro18v5_all_questions_en.exm *NP15_LOG_FILE_MANAGEMENT_02]

Question 4: Correct

Consider the following log message generated on a router:

*Aug 8 11:18:12.081: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down

What facility generated this message?

- UPDOWN
- FastEthernet0/0
- -5-
- %LINEPROTO

Explanation

The default log message format is as follows:

*Aug 8 11:18:12.081: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down

The components that comprise the log message include the following:

Component	Description
Timestamp	Indicates when the message was generated. In this example: *Aug 8 11:18:12.081:
Facility	Identifies the facility that created the message. In this example: %LINEPROTO
Severity Level	Indicates the severity level of the message. In this example: -5-
Mnemonic	Provides a mnemonic to help the administrator quickly identify the nature of the message. In this example: UPDOWN:
Message Text	Provides a description of the event. In this example: Line protocol on Interface FastEthernet0/0, changed state to down

References

LabSim for Network Pro, Section 15.7.
[netpro18v5_all_questions_en.exm NP15_LOG_FILE_MANAGEMENT_01]