Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/18/2022 7:39:24 pm • Time spent: 02:16

Score: 70% Passing Score: 80%

Question 1: ✔ Correct

Which two types of service accounts must you use to set up event subscriptions?

- [x] Default machine account
- [ ] Network server machine account
- [ ] Collector computer account
- [x] Specific user service account
- [ ] Local event administrators account

EXPLANATION

You would choose a default machine account and specific user service account. Either type of account must be a member of either the Source Computers Event Log Readers group (the most secure choice) or a member of the Local Administrators group.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_account_secp7.question.fex

Question 2: ✔ Correct

By default, events received from the source computers in Event Subscription are saved in which log?

- System log
- Application log
- Forwarded Events log
- Security log

EXPLANATION

By default, events received from source computers are saved in the Forwarded Events log.

There are application security logs, event security logs, and security logs for specialty applications, such as IDS/IPS, endpoints, firewalls, routers, and switches.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_event_secp7.question.fex

Question 3: ✔ Correct

You set up Event Subscription, but you are getting an overwhelming amount of events recorded. What should you do?

- Use the Runtime Status link
- Use the default machine account
- Choose the correct subscription type
- ➡ Define a filter

EXPLANATION

You would choose define a filter. If a filter is not defined, all events are collected.

Subscription type is required, but it does not influence the amount of events collected.

Using the Runtime Status link only verifies communications are working.

Using the default machine account is useful for the type of service account, but does not influence the amount of events collected.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_filter_secp7.question.fex

Question 4: ✕ Incorrect

Which of the following are required to configure Event Subscription for event forwarding? (Select three.)

- [x] Create a Windows firewall exception for HTTP or HTTPS on all source computers.
- [x] ~~Give the subscription a name.~~
- [x] Start Windows Event Collector service on collector computer.
- [ ] Configure Runtime Status.
- [ ] Configure the destination log.
- [ ] Create a filter.
- [ ] Start Windows Remote Management service on both the source and collector computers.

EXPLANATION

You must configure both the source and collector computers for event forwarding:

- On the source and collector computers, start Windows Remote Management service.
- On the collector computer, start the Windows Event Collector service.
- On the source computers, configure a Windows firewall exception for HTTP or HTTPS.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_forward_secp7.question.fex

Question 5: ✕ Incorrect

You are configuring a source-initiated subscription on the collector computer in Event Viewer. Which of the following do you need to specify?

- Computer group
- Content filter
- System log
- ~~Computer~~

EXPLANATION

You would choose the computer group for a source-initiated subscription.

Selecting a computer would be for the collector-initiated subscription.

The Forwarded Events log is selected, not the System log.

Content filtering is a strategy to keep employees from accessing unauthorized content on the web.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_group_secp7.question.fex

Question 6: ✕ Incorrect

For some reason, your source computers are not communicating properly with the collector. Which tool would you use to verify communications?

- Run **wecutil qc**
- Runtime Status
- ~~Run **winrm qc -q**~~
- Event Viewer System log

EXPLANATION

You would choose Runtime Status to verify communications after you have created a subscription.

The **wecutil qc** command would simply run the Windows Event Collector service.

The **winrm qc -q** command would initiate the Windows Remote Management service.

The Event Viewer System log would not verify current communications.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_runtime_secp7.question.fex

Question 7: ✔ Correct

For source-initiated subscriptions, which tool do you use to configure event forwarding?

- Group Policy
- Service account
- Filter settings
- Event Viewer

EXPLANATION

You should use Group Policy and use the Configure Target Subscription Manager Group Policy setting.

The service account only provides permissions to run properly.

Event forwarding settings for source-initiated subscriptions are unavailable in Event Viewer.

Filters define what is collected. They do not enable and configure event forwarding.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_source_01_secp7.question.fex

Question 8: ✔ Correct

You have a large number of source computers in your IT environment. Which subscription type would be most efficient to employ?

- Event forwarding
- Source-initiated
- Collector-initiated
- HTTP or HTTPS

EXPLANATION

You would choose source-initiated since there are a large number of source computers.

Collector-initiated is more efficient if you have a limited number of source computers.

Event forwarding uses HTTP to transfer the events from the source to the collector.

HTTP or HTTPS makes setup relatively easy because most firewalls are already configured for HTTP and HTTPS traffic.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_source_02_secp7.question.fex

Question 9: ✔ Correct

You want to set up a collector-initiated environment for event subscriptions. Which commands would you run? (Select two.)

- [ ] Run **winrm qc -q** on the collector computer.
- [x] Run **wecutil qc** on the collector computer.
- [x] Run **winrm qc -q** on the source computer.
- [ ] Run **winrm qc /q** on the collector computer.
- [ ] Run **wecutil qc /q** on the source computer
- [ ] Run **wecutil qc** on the source computer

EXPLANATION

To set up a collector-initiated environment for event subscriptions:

1. Run **winrm qc -q** on the source computer.
2. Add the collector computer account to the local Event Log Readers group on the source computer.
3. Add a user with admin privileges to the local Event Log Readers group on the source computer.
4. Run **wecutil qc** on the collector computer.

You must also run **winrm qc** on the collector computer. This command uses delivery optimization options other than the default.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_subscript_secp7.question.fex

Question 10: ✔ Correct

You wish to configure collector-initiated event subscriptions. On the collector computer, in which program do you configure a subscription?

- Computer Management
- Device Manager
- Local Group Policy
- ➡ Event Viewer

EXPLANATION

Event Viewer is used to configure collector-initiated subscriptions.

Collector-initiated event subscriptions are not configured using Group Policy like source-initiated subscriptions.

Device Manager offers no settings to configure event subscriptions.

Computer Management offers no settings to configure event subscriptions.

REFERENCES

12.4.4 Windows Event Subscriptions Facts

q_win_log_viewer_secp7.question.fex