

## 23: Lab 23: Assisted - Configuring system monitoring

Security+ (Exam SY0-701)

Solve



Congratulations, you passed!

Duration: 23 minutes, 27 seconds

☒ **confirm if the output of a wnmr command includes "10.1.16.1"**

Score: 1

Select the **Score** button to validate this task:

Value matched ...

Task complete

☒ **confirm if the output of Get-NetFirewallRule commands include "Allow"**

Score: 1

Select the **Score** button to validate this task:

Values matched ...

Task complete

☒ What types of centralized logging management are available on Windows? (Select two)

Score: 1

- ☒ Collector initiated
- ☐ Domain controller initiated
- ☐ Sysconfig initiated
- ☒ Source computer initiated
- ☐ Client initiated

Congratulations, you have answered the question correctly.

☒ Where in the Event Viewer can you view the events from a remote system?

Score: 1

- ☐ Application log
- ☐ Security log
- ☐ Setup log
- ☐ System log
- ☒ Forwarded Events

Congratulations, you have answered the question correctly.

☒ On an event pulled from the remote system, what was listed as the Computer: value?


Score: 1

- ☐ DC10
- ☐ DC10.ad.structureality.com
- ☐ MS10

☒ MS10.ad.structureality.com

Congratulations, you have answered the question correctly.

✓ What systems can be configured as a collecting system through the Windows Event Viewer *Score: 1*  
Subscription...

-  ☒ any domain member  
☐ only domain controllers  
☐ only servers  
☐ Linux clients

Congratulations, you have answered the question correctly.

✓ The ability to use centralized logging in Windows is enabled and configure by default. *Score: 1*

- ☐ True  
☒ False

Congratulations, you have answered the question correctly.

