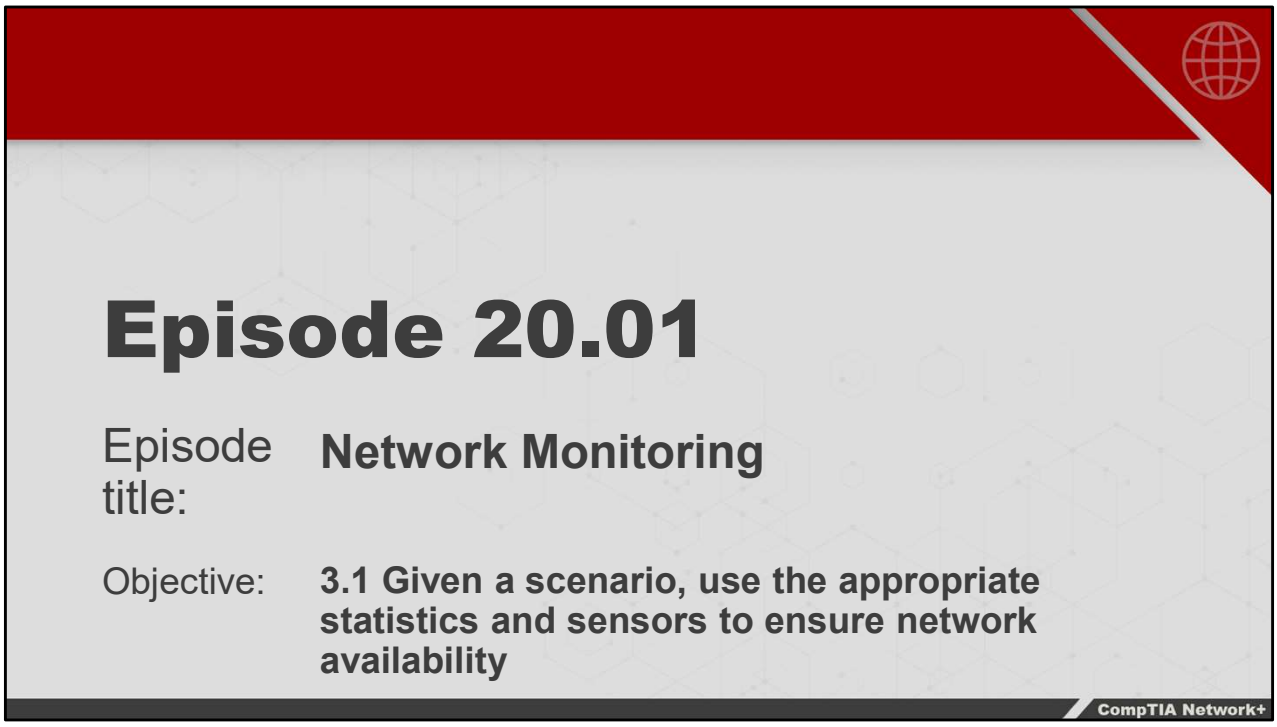
Chapter 20

Network Monitoring

CompTIA Network+


Episode 20.01
Episode title:
Network Monitoring
Objective:
3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability
CompTIA Network+

L3s

- Performance metrics
- Network metrics
- Environmental factors
- Interface statistics/status
- Link state
- Speed and duplex factors
- Send and receive traffic
- Cyclic Redundancy Check (CRC) errors

L3s

- Giants and runts
- Encapsulation errors
- Byte counts
- Zabbix Dashboard
- LibreNMS
- Grafana
- SolarWinds

Quick Review

- Networks must be monitored in a number of ways including performance, traffic, and environmental
- Giants and runts refer to the packet size
- Various network management systems (NMS) include Zabbix, LibreNMS, Grafana, and SolarWinds


Episode 20.02
Episode title:
SNMP
Objective:
1.5 Explain common ports and protocols, their application, and encrypted alternatives
3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability
4.3 Given a scenario, apply network hardening techniques
CompTIA Network+

L3s

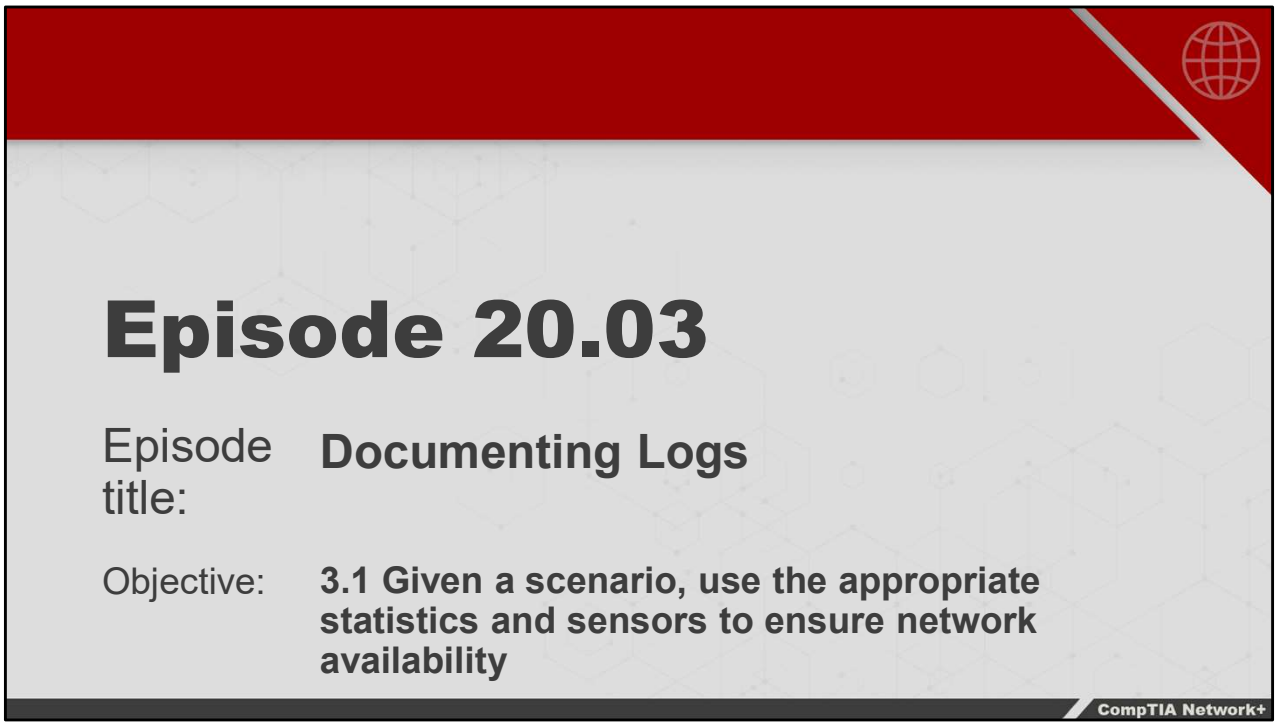
- Simple Network Management Protocol (SNMP)
- SNMP version 1 does not support encryption
- SNMP version 2 added basic encryption
- SNMP version 3 added TLS
- An SNMP community is an organization of managed devices

L3s

- Cacti is an open-source NMS for graphing SNMP data
- A few to look at are Nagios, Zabbix, and Spiceworks

Quick Review

- SNMP uses UDP port 161 or port 10161 when using TLS
- SNMP managed devices run an agent that talks with a network management station (NMS)
- SNMPv1 is unencrypted, SNMPv2 added basic encryption, SNMPv3 added TLS

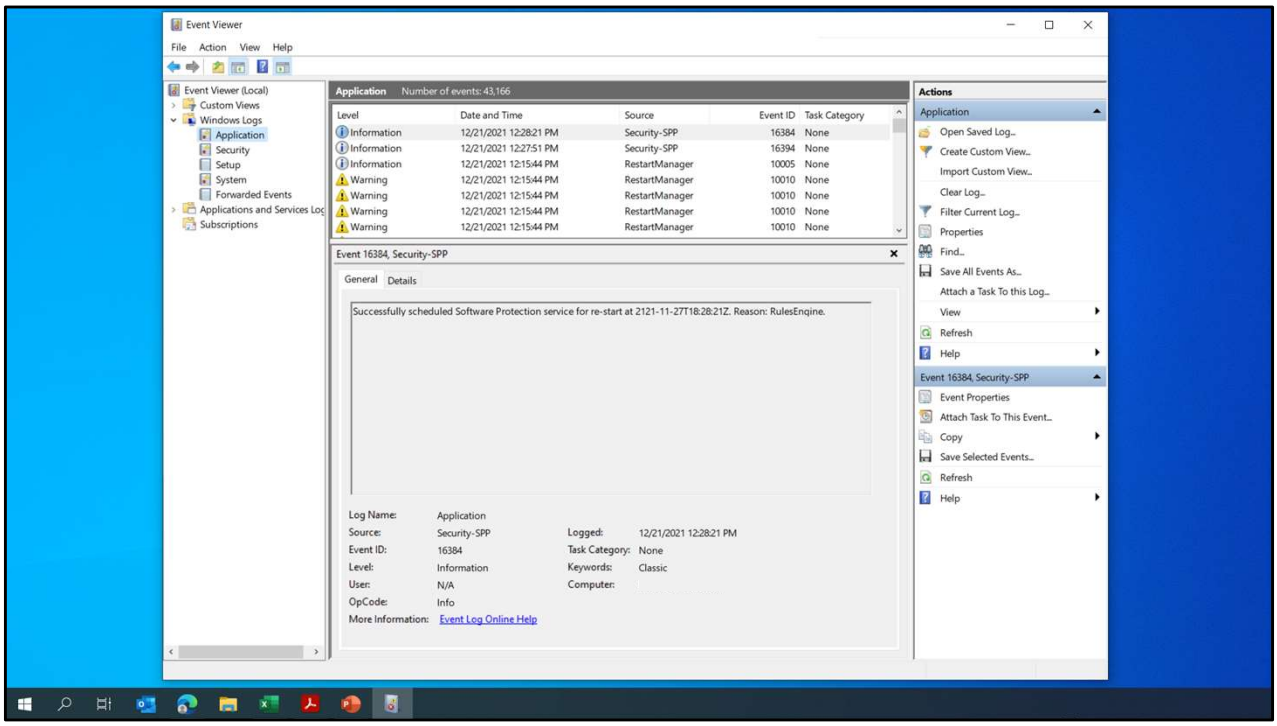

Episode 20.03
Episode title:
Documenting Logs
Objective:
3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability
CompTIA Network+

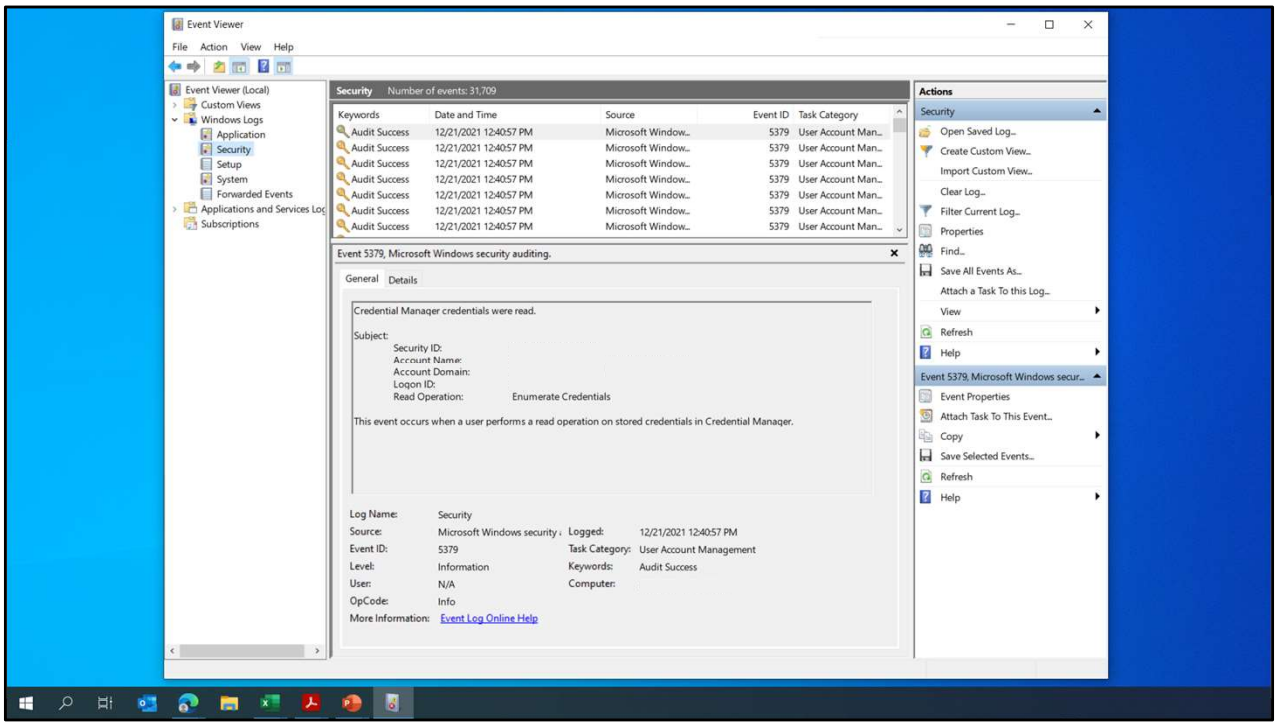
L3s

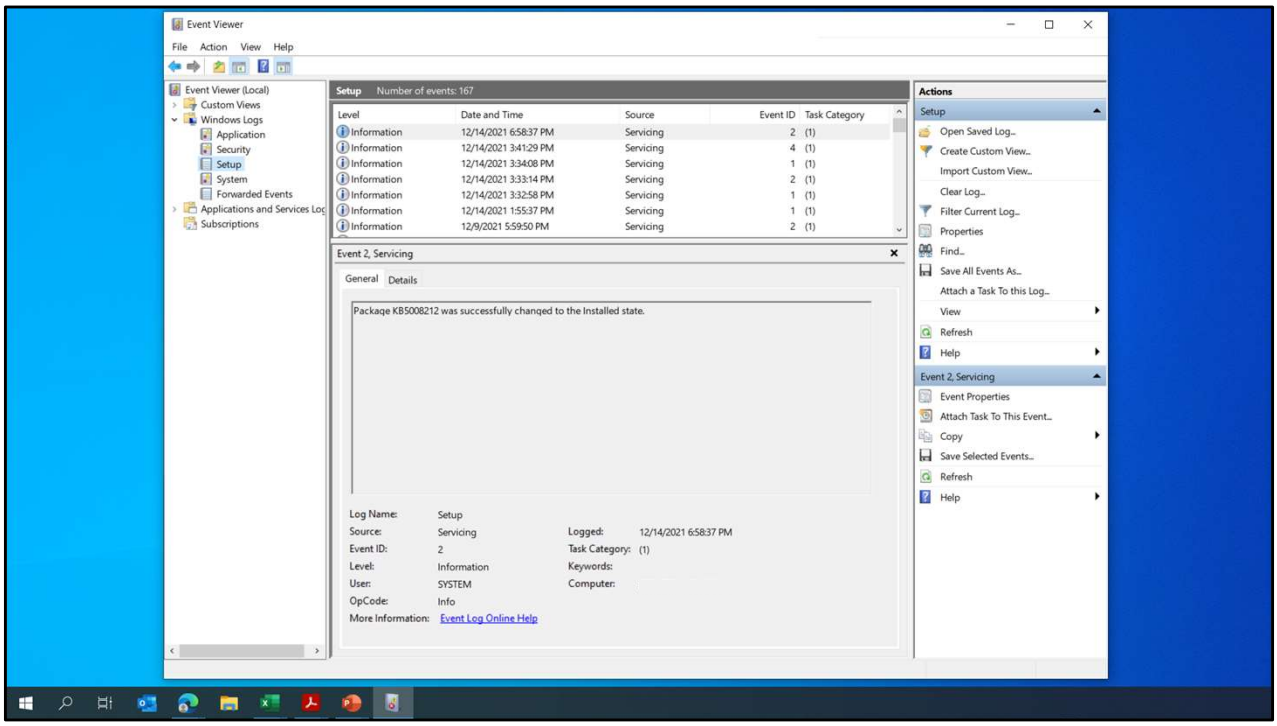
- One more thing: Colombo was a TV show in the 1970s
- System of general logs
- Event Viewer
- Application logs
- Security logs
- System logs

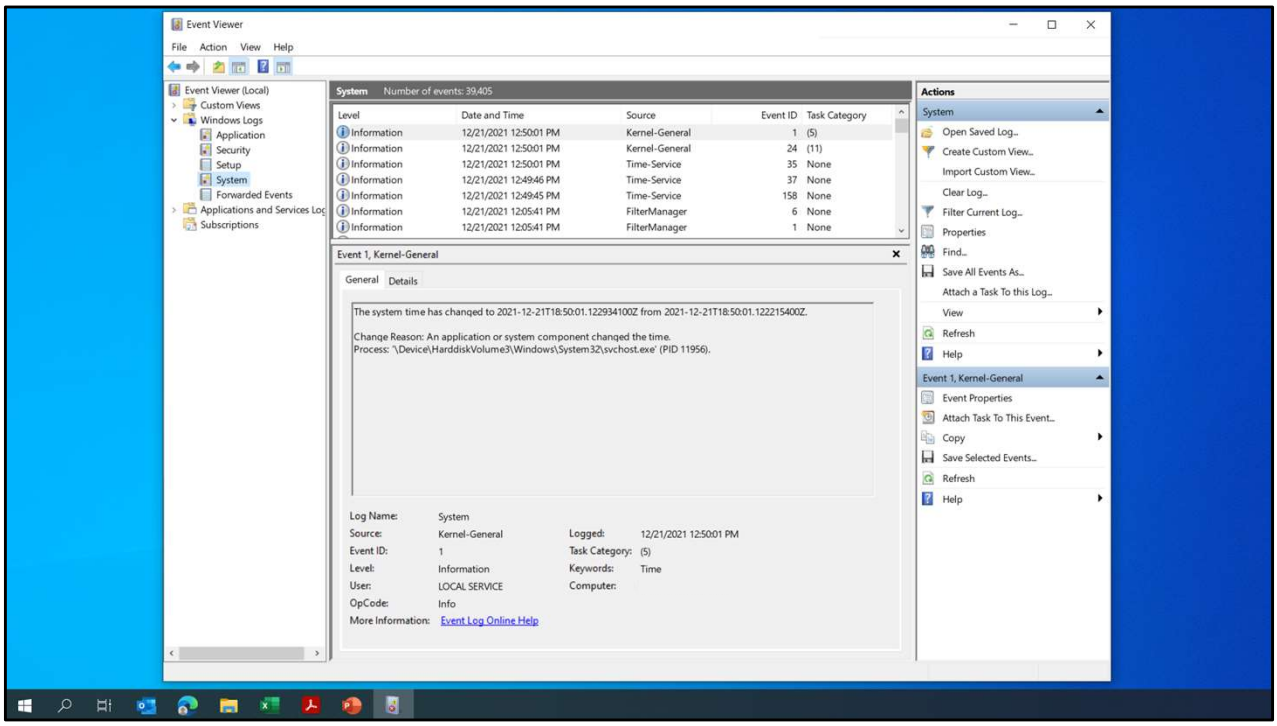
L3s

- Simple Network Management Protocol (SNMP)
- Syslog
- Syslog errors go from 0 to 7
- History log
- Change log

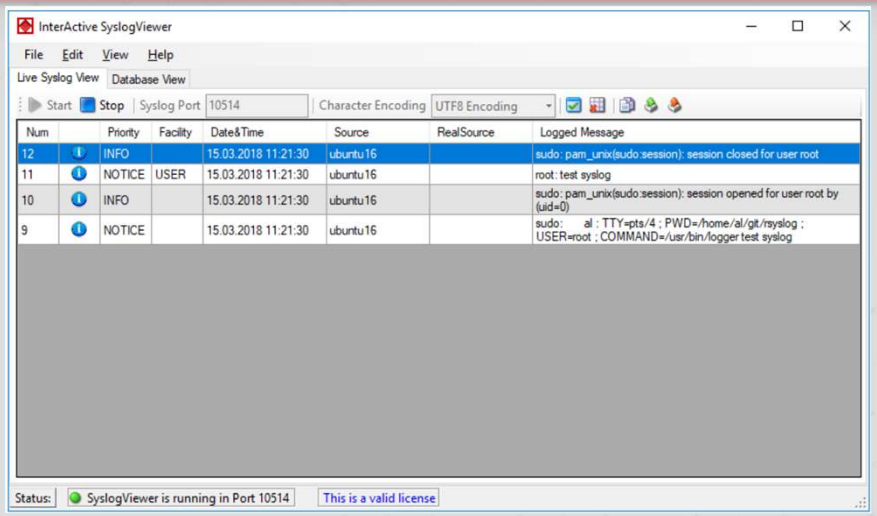

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
Application Number of events: 43,166
Level Date and Time Source Event ID Task Category
Information 12/21/2021 12:28:21 PM Security-SPP 16384 None
Information 12/21/2021 12:27:51 PM Security-SPP 16394 None
Information 12/21/2021 12:15:44 PM RestartManager 10005 None
Warning 12/21/2021 12:15:44 PM RestartManager 10010 None
Warning 12/21/2021 12:15:44 PM RestartManager 10010 None
Warning 12/21/2021 12:15:44 PM RestartManager 10010 None
Warning 12/21/2021 12:15:44 PM RestartManager 10010 None
Event 16384, Security-SPP
General Details
Successfully scheduled Software Protection service for re-start at 2121-11-27T18:28:21Z. Reason: RulesEngine.
Log Name: Application
Source: Security-SPP
Logged: 12/21/2021 12:28:21 PM
Event ID: 16384
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer:
OpCode: Info
More Information: Event Log Online Help
Actions
Application
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 16384, Security-SPP
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
Security Number of events: 31,709
Keywords Date and Time Source Event ID Task Category
Audit Success 12/21/2021 12:40:57 PM Microsoft Window... 5379 User Account Man...
Event 5379, Microsoft Windows security auditing.
General Details
Credential Manager credentials were read.
Subject:
Security ID:
Account Name:
Account Domain:
Logon ID:
Read Operation: Enumerate Credentials
This event occurs when a user performs a read operation on stored credentials in Credential Manager.
Log Name: Security
Source: Microsoft Windows security
Logged: 12/21/2021 12:40:57 PM
Event ID: 5379
Task Category: User Account Management
Level: Information
Keywords: Audit Success
User: N/A
Computer:
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 5379, Microsoft Windows secur...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
Setup Number of events: 167
Level Date and Time Source Event ID Task Category
Information 12/14/2021 6:58:37 PM Servicing 2 (1)
Information 12/14/2021 3:41:29 PM Servicing 4 (1)
Information 12/14/2021 3:34:08 PM Servicing 1 (1)
Information 12/14/2021 3:33:14 PM Servicing 2 (1)
Information 12/14/2021 3:32:58 PM Servicing 1 (1)
Information 12/14/2021 1:55:37 PM Servicing 1 (1)
Information 12/9/2021 5:59:50 PM Servicing 2 (1)
Event 2, Servicing
General Details
Package KB5008212 was successfully changed to the Installed state.
Log Name: Setup
Source: Servicing
Logged: 12/14/2021 6:58:37 PM
Event ID: 2
Task Category: (1)
Level: Information
Keywords:
User: SYSTEM
Computer:
OpCode: Info
More Information: Event Log Online Help
Actions
Setup
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 2, Servicing
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
System Number of events: 39,405
Level Date and Time Source Event ID Task Category
Information 12/21/2021 12:50:01 PM Kernel-General 1 (5)
Information 12/21/2021 12:50:01 PM Kernel-General 24 (11)
Information 12/21/2021 12:50:01 PM Time-Service 35 None
Information 12/21/2021 12:49:46 PM Time-Service 37 None
Information 12/21/2021 12:49:45 PM Time-Service 158 None
Information 12/21/2021 12:05:41 PM FilterManager 6 None
Information 12/21/2021 12:05:41 PM FilterManager 1 None
Event 1, Kernel-General
General Details
The system time has changed to 2021-12-21T18:50:01.122934100Z from 2021-12-21T18:50:01.122215400Z.
Change Reason: An application or system component changed the time.
Process: '\Device\HarddiskVolume3\Windows\System32\svchost.exe' (PID 11956).
Log Name: System
Source: Kernel-General
Logged: 12/21/2021 12:50:01 PM
Event ID: 1
Task Category: (5)
Level: Information
Keywords: Time
User: LOCAL SERVICE
Computer:
OpCode: Info
More Information: Event Log Online Help
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 1, Kernel-General
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help

InterActive Syslog Viewer



Source: https://www.adiscon.com/files/pdf/SyslogViewer.pdf

Quick Review

- Review the different types of logs
- Event Viewer is a Windows tool that displays various types of logs
- Many UNIX systems use syslogs, which works with SNMP


Episode 20.04
Episode title:
System Monitoring
Objective:
3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability
CompTIA Network+

L3s

- Error rate
- Utilization
- Notification
- Packet drops
- Bandwidth
- File integrity

Quick Review

- Abnormal warnings of high error rate or utilization might signify security breaches or broken equipment
- A baseline helps identify irregular activity that needs to be investigated
- File integrity is an important part of a monitoring program


Episode 20.05
Episode title:
Security Information and Event Management (SIEM)
Objective:
4.1 Explain common security concepts
CompTIA Network+

L3s

- Security information and event management (SIEM)
- Aggregation
- Correlation
- Logs
- Write once, read many (WORM)

Correlation

- Alerts
  - For notification if something goes bad
- Triggering
  - Exceeding thresholds

Quick Review

- SIEM tools aggregate and correlate data, allowing organization into valuable information
- A SIEM tool accesses and correlates across logs to review an event
- SIEMs have alerts and the ability to notify based on a configurable trigger