

# Microsoft® Official Course



Module12

Monitoring Server Performance

**Microsoft®**

# Module Overview

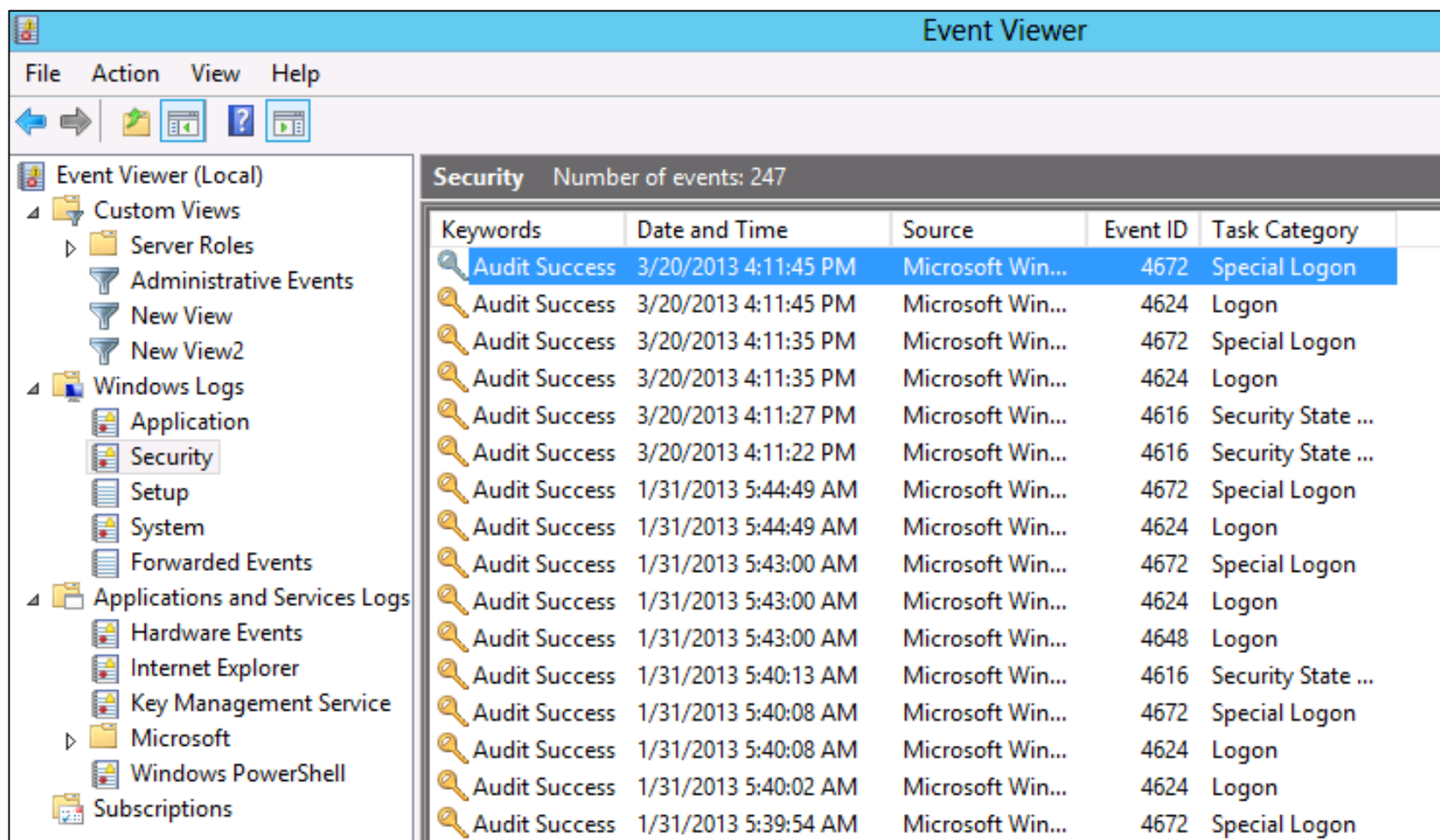
- Event Logging
- Performance Monitoring

# Lesson 1: Event Logging

- Windows Logs
- Application and Services Logs
- What Are the Event Types and Data Formats?
- Filters, Custom Views, Tasks, and Subscriptions
- Demonstration: How to Use the Event Viewer

# Windows Logs

- Event Viewer can display Windows Logs

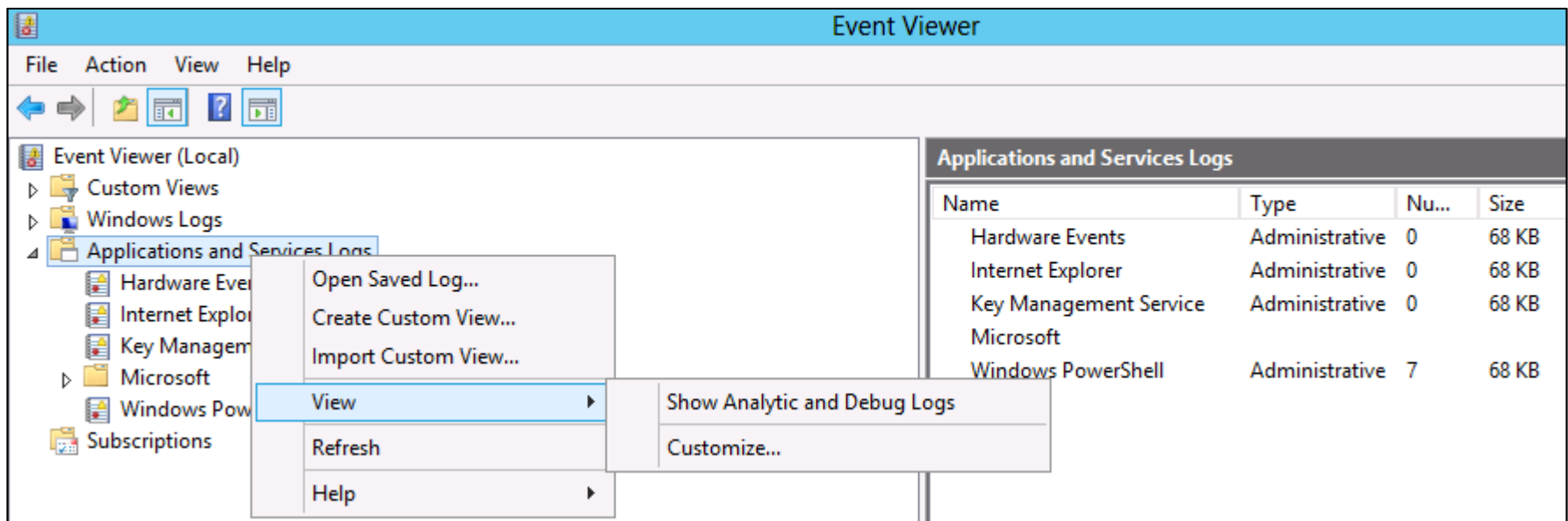


The screenshot shows the Windows Event Viewer application. The left-hand pane displays a tree view of event logs, with 'Security' selected under 'Windows Logs'. The right-hand pane shows a list of 247 security events. The top row is highlighted in blue.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	3/20/2013 4:11:45 PM	Microsoft Win...	4672	Special Logon
Audit Success	3/20/2013 4:11:45 PM	Microsoft Win...	4624	Logon
Audit Success	3/20/2013 4:11:35 PM	Microsoft Win...	4672	Special Logon
Audit Success	3/20/2013 4:11:35 PM	Microsoft Win...	4624	Logon
Audit Success	3/20/2013 4:11:27 PM	Microsoft Win...	4616	Security State ...
Audit Success	3/20/2013 4:11:22 PM	Microsoft Win...	4616	Security State ...
Audit Success	1/31/2013 5:44:49 AM	Microsoft Win...	4672	Special Logon
Audit Success	1/31/2013 5:44:49 AM	Microsoft Win...	4624	Logon
Audit Success	1/31/2013 5:43:00 AM	Microsoft Win...	4672	Special Logon
Audit Success	1/31/2013 5:43:00 AM	Microsoft Win...	4624	Logon
Audit Success	1/31/2013 5:43:00 AM	Microsoft Win...	4648	Logon
Audit Success	1/31/2013 5:40:13 AM	Microsoft Win...	4616	Security State ...
Audit Success	1/31/2013 5:40:08 AM	Microsoft Win...	4672	Special Logon
Audit Success	1/31/2013 5:40:08 AM	Microsoft Win...	4624	Logon
Audit Success	1/31/2013 5:40:02 AM	Microsoft Win...	4624	Logon
Audit Success	1/31/2013 5:39:54 AM	Microsoft Win...	4672	Special Logon

# Application and Services Logs

- Application and Server Logs are primarily used for local Administration and Operational events and logs are typically created for each role added.
- By default, Analytic and Debug logs are disabled and hidden



# What Are the Event Types and Data Formats?

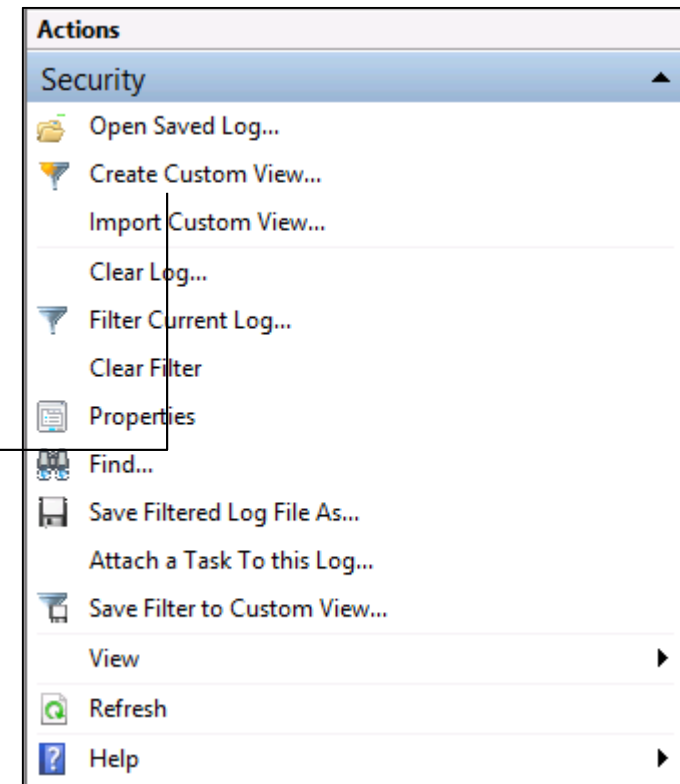
- Level Types occurring in Logs
  - Information
  - Error
  - Warning
- Additional classification occurring in Security Log
  - Audit Failure
  - Audit Success
- Events are presented in the same format for both Windows Logs and Application and Services Logs

# Filters, Custom Views, Tasks, and Subscriptions

- Filters, Custom Views, Tasks, and Subscriptions help you focus on specific types of events

The 'Create Custom View' dialog box is shown with the 'Filter' tab selected. It contains the following fields and options:

- Logged:** A dropdown menu set to 'Any time'.
- Event level:** Checkboxes for 'Critical', 'Warning', 'Verbose', 'Error', and 'Information'.
- By log:** A radio button that is selected, with a dropdown menu for 'Event logs'.
- By source:** A radio button that is unselected, with a dropdown menu for 'Event sources'.
- Includes/Excludes Event IDs:** A text box containing '<All Event IDs>' with a small instruction below it: 'Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76'.
- Task category:** A dropdown menu.
- Keywords:** A dropdown menu.
- User:** A dropdown menu set to '<All Users>'.
- Computer(s):** A dropdown menu set to '<All Computers>'.
- Buttons:** 'Clear', 'OK', and 'Cancel'.

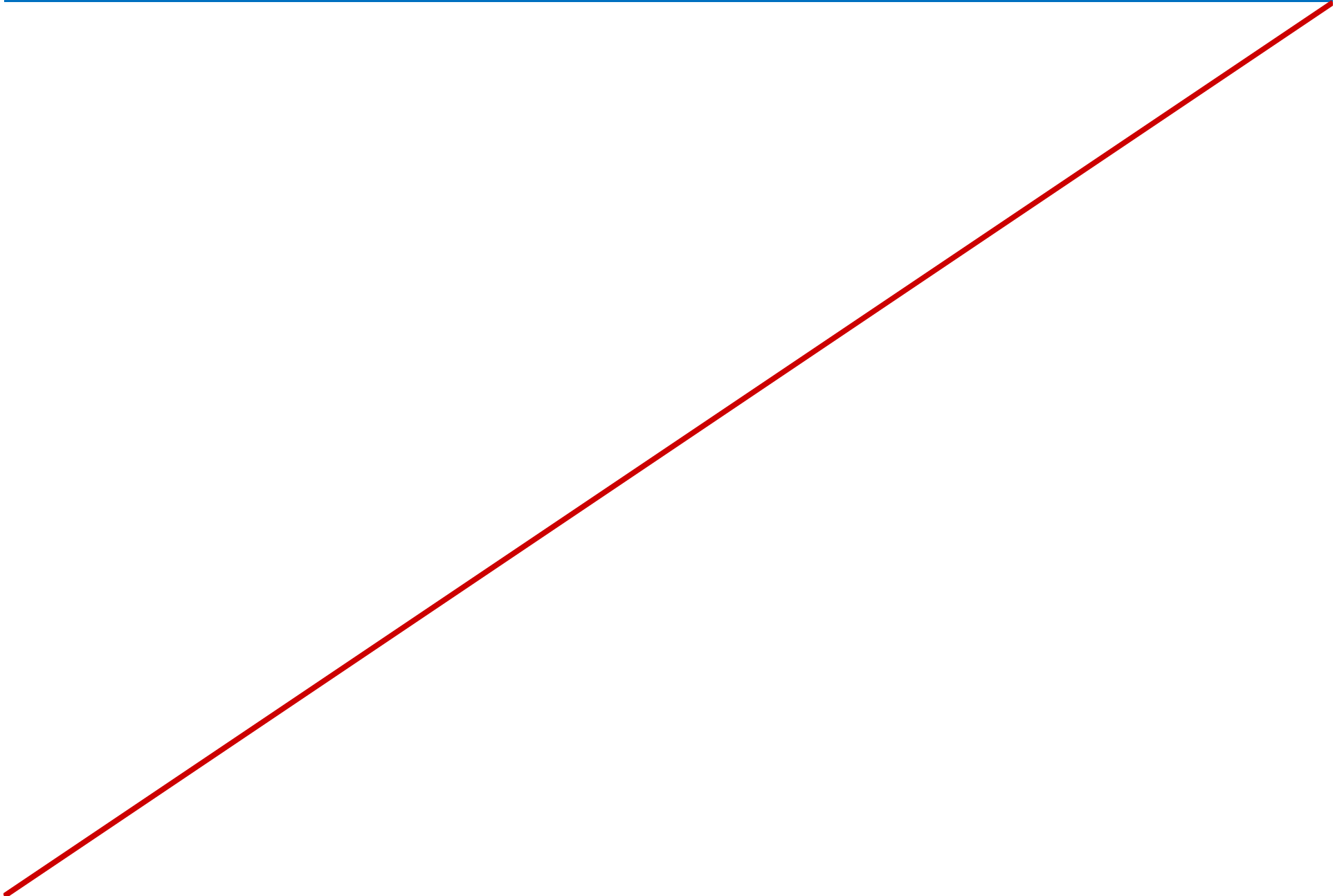


# Demonstration: How to Use the Event Viewer

- In this demonstration, you will see how to use the Event Viewer to review Windows Logs, and Application and Services Logs. You will also see how to create a custom view.



Notes Page Over-flow Slide. Do Not Print Slide.



## Lesson 2: Performance Monitoring

- Performance Bottlenecks
- The Process of Performance Monitoring
- Performance Counters
- Demonstration: How to Capture Current Performance Activity
- What Are Data Collector Sets?
- Demonstration: How to Use Data Collector Sets to Capture Performance Data
- Demonstration: How to Use Alerts to Identify Performance Bottlenecks

# Performance Bottlenecks

- A performance bottleneck occurs when a server is unable to service a request for a resource
- There are many situations where bottlenecks can occur
- There are many bottleneck mitigation strategies
  - Adding and upgrading resources
  - Balancing users and processes across multiple servers
  - Running resource intensive applications during non-peak periods
  - Configuring resources for best performance

# The Process of Performance Monitoring

## Real Time

- Performance monitoring
- Service level agreements

## Historical

- Event logs
- Retained performance logs

## Tools

- Event Viewer
- Windows System Resource Manager
- Network Monitor
- Performance Monitor
- Resource Monitor
- System Center Operations Manager
- Task Manager

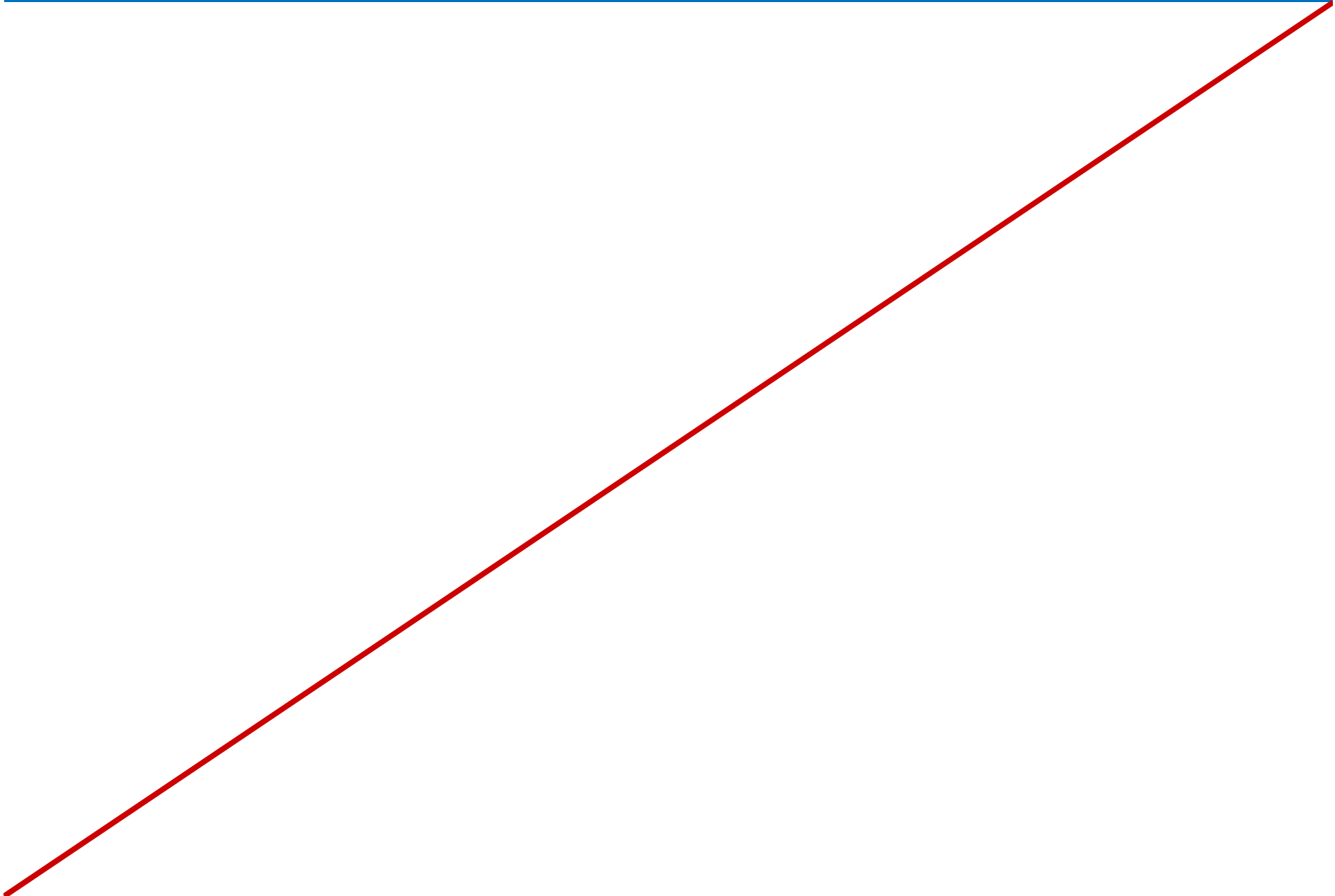
# Performance Counters

- Primary Processor Counters
  - % Processor Time
  - Interrupts per Second
  - Processor Queue Length
- Primary Memory Counters
  - Pages per Second
- Primary Disk Counters
  - % Disk Time
  - Average Disk Queue Length
- Primary Network Counters

## Demonstration: How to Capture Current Performance Activity

- In this demonstration, you will see how to use Performance Monitor to view real-time performance data

Notes Page Over-flow Slide. Do Not Print Slide.



# What Are Data Collector Sets?

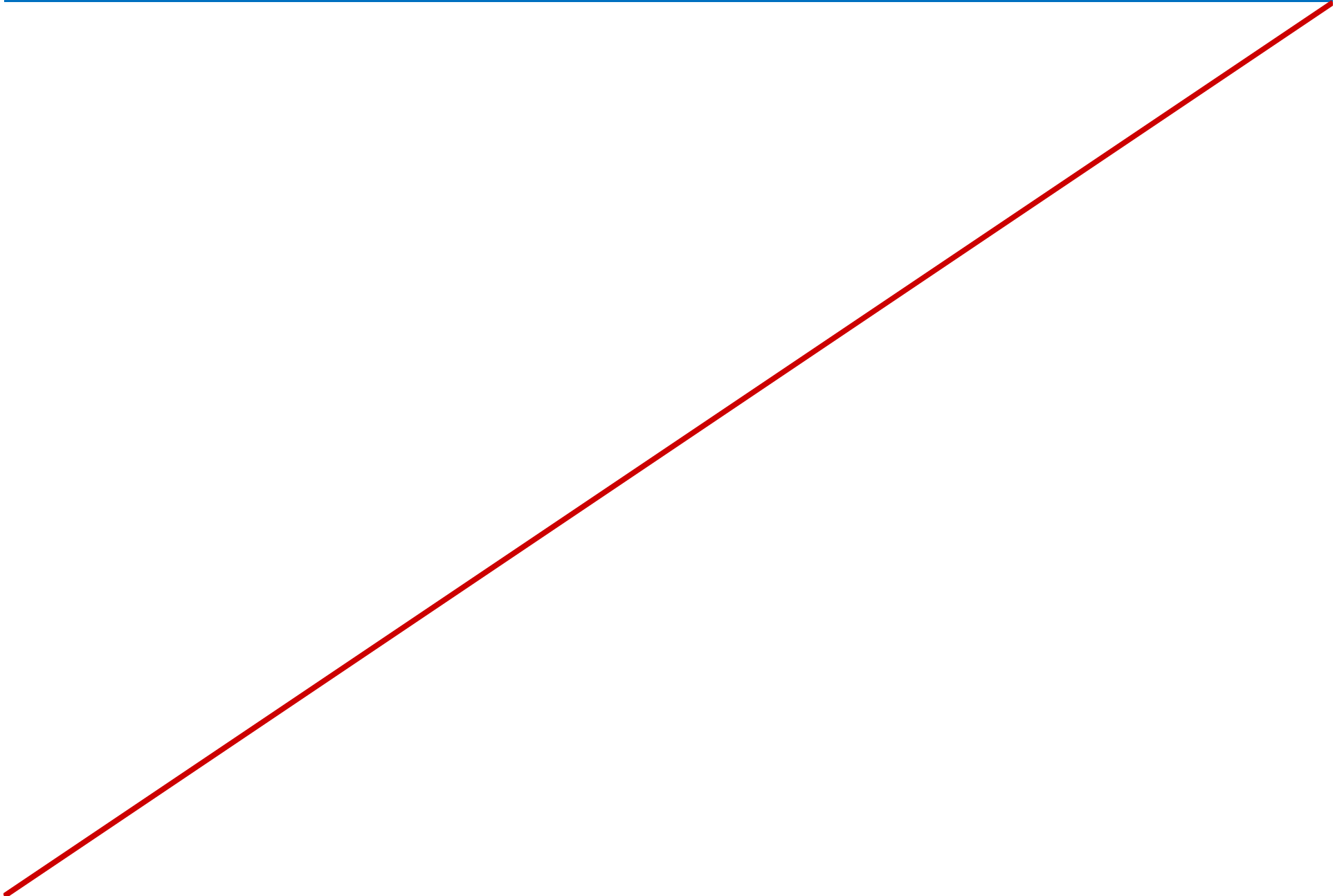
- Data Collector Sets enable you to gather performance-related and other system statistics for analysis
- Data Collector Sets can contain the following types of data collectors:
  - Performance counters
  - Event trace data
  - System configuration information



## Demonstration: How to Use Data Collector Sets to Capture Performance Data

- In this demonstration, you will see how to collect performance data in a Data Collector Set

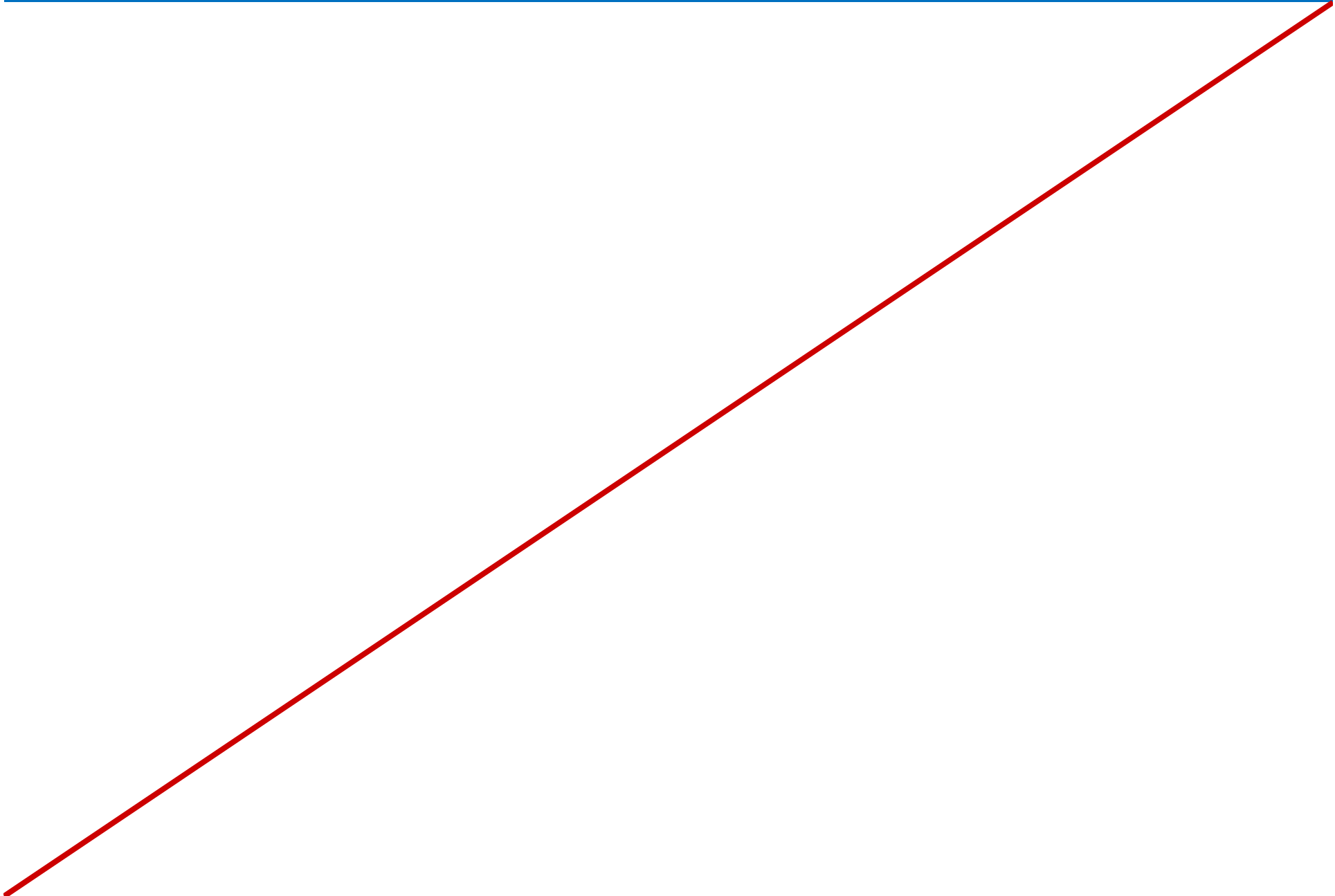
Notes Page Over-flow Slide. Do Not Print Slide.



## Demonstration: How to Use Alerts to Identify Performance Bottlenecks

- In this demonstration, you will see how to create an alert and verify it generates an Event when the alert is triggered.

Notes Page Over-flow Slide. Do Not Print Slide.



# Lab: Monitoring Server Performance

- Exercise 1: Creating a Performance Baseline
- Exercise 2: Simulating a Server Load
- Exercise 3: Determining Probable Performance Bottlenecks
- Exercise 4: Create, test, and verify an alert

## Logon Information

Virtual Machines: 10967A-LON-DC1, 10967A-LON-SVR1

User Name: ADATUM\Administrator

Password: Pa\$\$w0rd

Estimated Time: 60 minutes

## Lab Scenario

You have successfully deployed some new servers at the A. Datum branch offices. Before the system goes live, you decide to establish a performance baseline so that you can compare future workloads to the expected workload and you also want to create and test an Alert that you can use to monitor the volume of data on the Network Interface on the server.

## Lab Review

- During the lab, you collected data in a Data Collector Set. What is the advantage of collecting data in this manner?
- What significant counters should you monitor in Windows Server Performance Monitor?

# Module Review and Takeaways

- Tools