# Lab: Monitoring and troubleshooting Windows Server

## Scenario

Contoso, Ltd is a global engineering and manufacturing company with its head office in Seattle, Washington, in the United States. An IT office and datacenter are in Seattle to support the Seattle location and other locations. Contoso recently deployed a Windows Server 2019 server and client infrastructure.

Because the organization deployed new servers, it's important to establish a performance baseline with a typical load for these new servers. You've been asked to work on this project. Additionally, to make the process of monitoring and troubleshooting easier, you decided to perform centralized monitoring of event logs.

## Objectives

After completing this lab, you'll be able to:

* Establish a performance baseline.
* Identify the source of a performance problem.
* Review and configure centralized event logs.

## Lab setup

Estimated time: **40 minutes**

Virtual machines: **WS-011T00A-SEA-DC1**, **WS-011T00A-SEA-ADM1**, and **WS-011T00A-SEA-CL1**

User name: \*\*Contoso\*

Password: **Pa55w.rd**

## Lab setup

1. Select **SEA-DC1**.
2. Sign in by using the following credentials:

* User name: **Administrator**
* Password: **Pa55w.rd**
* Domain: **Contoso**

1. Repeat these steps for **SEA-ADM1** and **SEA-CL1**.

## Exercise 1: Establishing a performance baseline

### Scenario

In this exercise, you'll use **Performance Monitor** on the server and create a baseline by using typical performance counters.

The main tasks for this exercise are:

1. Create and start a data collector set
2. Create a typical workload on the server
3. Analyze the collected data

**Note**: After starting the Data Collector Set, there might be a delay of 10 minutes for the results to appear.

### Task 1: Create and start a data collector set

1. Switch to **SEA-ADM1**.
2. Open **Performance Monitor**.
3. Create a new **User Defined** data collector set by using the following information to complete the process:

* Name: **SEA-ADM1 Performance**
* Create: **Create manually (Advanced)**
* Type of data: **Performance counter**
* Select the following counters (using all default instances):
  + **Memory/sec**
  + **Network InterfaceTotal/sec**
  + **PhysicalDisk\% Disk Time**
  + **PhysicalDisk. Disk Queue Length**
  + **Processor\% Processor Time**
  + **SystemQueue Length**
* Sample interval: **1** second
* Where to store data: default value

1. Save and close the data collector set.
2. In **Performance Monitor**, in the results pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Start**.

### Task 2: Create a typical workload on the server

1. Open a **Command Prompt** window, and then run the following commands by selecting Enter after each command:

* Fsutil file createnew bigfile 104857600  
  Copy bigfile \\SEA-dc1\c$  
  Copy \\SEA-dc1\c$\bigfile bigfile2  
  Del bigfile\*.\*  
  Del \\SEA-dc1\c$\bigfile\*.\*

1. Don't close the **Command Prompt** window.

### Task 3: Analyze the collected data

1. Switch to **Performance Monitor**.
2. Stop the **SEA-ADM1 Performance** data collector set.
3. In **Performance Monitor**, in the navigation pane, browse to **Reports**, **User Defined**, **SEA-ADM1**, **SEA-ADM1\_DateTime-000001**, and then review the report data. Use the Report view.
4. Record the values that are listed in the report for later analysis. Recorded values include:

* **Memory/sec**
* **Network InterfaceTotal/sec**
* **PhysicalDisk% Disk Time**
* **PhysicalDisk. Disk Queue Length**
* **Processor% Processor Time**
* **SystemQueue Length**

### Results

After this exercise, you should have established a baseline for performance-comparison purposes.

## Exercise 2: Identifying the source of a performance problem

### Scenario

In this exercise, you'll simulate a load to represent the system in live usage, gather performance data by using your data collector set, and then determine the potential cause of the performance problem.

The main tasks for this exercise are:

1. Create additional workload on the server
2. Capture performance data by using a data collector set
3. Remove the workload, and then review the performance data

### Task 1: Create additional workload on the server

1. On **SEA-ADM1**, open File Explorer.
2. Browse to the **C:11** folder.
3. On **SEA-ADM1**, run **CPUSTRES64**.
4. Configure the first highlighted task to run **BUSY (75%)**.

### Task 2: Capture performance data by using a data collector set

1. Switch to **Performance Monitor**.
2. In **Performance Monitor**, browse to **Data Collector Sets**, **User Defined**, and then in the results pane, start the **SEA-ADM1 Performance** data collector set.
3. Wait a minute to allow the data capture to occur.

### Task 3: Remove the workload, and then review the performance data

1. Close CPUSTRES64, and then close File Explorer.
2. Switch to **Performance Monitor**.
3. Stop the **SEA-ADM1 Performance** data collector set.
4. In **Performance Monitor**, in the navigation pane, browse to **Reports**, **User Defined**, **SEA-ADM1**, **SEA-ADM1\_DateTime-000002**, and then review the report data. Record the following values:
   * **Memory/sec**
   * **Network InterfaceTotal/sec**
   * **PhysicalDisk% Disk Time**
   * **PhysicalDisk. Disk Queue Length**
   * **Processor% Processor Time**
   * **SystemQueue Length**

### Results

After this exercise, you should have used performance tools to identify a potential performance bottleneck.

### Exercise 3: Viewing and configuring centralized event logs

### Scenario

In this exercise, you'll use **SEA-DC1** to collect event logs from **SEA-ADM1**. Specifically, you'll use this process to gather performance-related alerts from your network servers.

The main tasks for this exercise are:

1. Configure subscription prerequisites
2. Create a subscription
3. Configure a performance counter alert
4. Introduce additional workload on the server
5. Verify the results
6. Prepare for the next module

### Task 1: Configure subscription prerequisites

1. Switch to **SEA-ADM1**.
2. At the command prompt, run **winrm quickconfig** to enable the administrative changes that are necessary on a source computer. As you can observe, the WinRM service is running and enabled for remote management already.
3. Add **SEA-CL1** to the local **Event Log Readers** group.
4. Switch to **SEA-CL1**.
5. Open a **Command Prompt** window, and then run **wecutil qc** to enable the administrative changes that are necessary on a collector computer.

### Task 2: Create a subscription

1. Open **Event Viewer**.
2. Create a new subscription with the following properties:
   * Computers: **SEA-ADM1**
   * Name: **SEA-ADM1 Events**
   * Collector: **initiated**
   * Events: **Critical**, **Warning**, **Information**, **Verbose**, and **Error**
   * Logged: **Last 7 days**
   * Logs: **Applications and Services Logs / Microsoft / Windows / Diagnosis-PLA / Operational**

### Task 3: Configure a performance counter alert

1. Switch to **SEA-ADM1**.
2. Open **Performance Monitor**.
3. Create a new **User Defined** data collector set by using the following information to complete the process:
   * Name: **SEA-ADM1 Alert**
   * Create: **Create manually (Advanced)**
   * Type of data: **Performance counter Alert**
   * Select the following counters: **Processor% Processor Time** above **10** percent
   * Sample interval: **1** second
   * Where to store data: default value
   * Alert action: **Log an entry in the application event log**
4. Start the **SEA-ADM1 Alert** data collector set.

### Task 4: Introduce additional workload on the server

1. On **SEA-ADM1**, open File Explorer.
2. Browse to the **C:11** folder.
3. On **SEA-ADM1**, run **CPUSTRES64**.
4. Configure the first highlighted task to run **BUSY (75%)**.

### Task 5: Verify the results

* Switch to **SEA-CL1**, and then open **Forwarded Events**. In **Performance Monitor**, are any performance-related alerts in the subscribed application log? Hint: They have an ID of 2031.

©2019 Microsoft Corporation. All rights reserved. The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are ***not*** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.