# Lab answer key: Monitoring and troubleshooting Windows Server

### Exercise 1: Establishing a performance baseline

**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. Select **Start**.
3. In the search box, enter **Perf**, and then in the **Best match** list, select **Performance Monitor**.
4. In **Performance Monitor**, expand **Data Collector Sets** in the navigation pane, and then select **User Defined**.
5. Right-click or access the context menu for **User Defined**, select **New**, and then select **Data Collector Set**.
6. In the **Create new Data Collector Set Wizard**, enter **SEA-ADM1 Performance** in the **Name** box.
7. Select **Create manually (Advanced)**, and then select **Next**.
8. On the **What type of data do you want to include?** page, select the **Performance counter** check box, and then select **Next**.
9. On the **Which performance counters would you like to log?** page, select **Add**.
10. In the **Available counters** list, expand **Processor**, select **% Processor Time**, and then select **Add**.
11. In the **Available counters** list, expand **Memory**, select **Pages/sec**, and then select **Add**.
12. In the **Available counters** list, expand **PhysicalDisk**, select **% Disk Time**, and then select **Add**.
13. Select **Avg. Disk Queue Length**, and then select **Add**.
14. In the **Available counters** list, expand **System**, select **Processor Queue Length**, and then select **Add**.
15. In the **Available counters** list, expand **Network Interface**, select **Bytes Total/sec**, select **Add**, and then select **OK**.
16. On the **Which performance counters would you like to log?** page, enter **1** in the **Sample interval** box, and then select **Next**.
17. On the **Where would you like the data to be saved?** page, select **Next**.
18. On the **Create the data collector set?** page, select **Save** and **close**, and then select **Finish**.
19. 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. Select **Start**, enter **Cmd** in the search box, and then select **Command Prompt** in the **Best match** list.
2. At the command prompt, enter the following command, and then select Enter:

* Fsutil file createnew bigfile 104857600

1. At the command prompt, enter the following command, and then select Enter:

* Copy bigfile \\SEA-dc1\c$

1. At the command prompt, enter the following command, and then select Enter:

* Copy \\SEA-dc1\c$\bigfile bigfile2

1. At the command prompt, enter the following command, and then select Enter:

* Del bigfile\*.\*

1. At the command prompt, enter the following command, and then select Enter:

* 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. In the navigation pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Stop**.
3. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, expand **SEA-ADM1 Performance**, select **SEA-ADM1\_DateTime-000001**, and then review the report data.
4. On the menu bar, select **Change graph type** or press Ctrl+G, and then select **Report**.
5. 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

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

1. On **SEA-ADM1**, open File Explorer.
2. Browse to **C:11**.
3. Double-click or select **CPUSTRES64.EXE**, and then select Enter.
4. In the **CPU Stress - Sysinternals: www.sysinternals.com** dialog box, right-click or access the context menu for the highlighted thread at the top of the list of running threads, select **Activity Level**, and then select **Busy (75%)**.

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

1. Switch to **Performance Monitor**.
2. In **Performance Monitor**, expand **Data Collector Sets**, and select **User Defined**.
3. In the results pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Start**.
4. Wait a minute to allow the data capture to occur.

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

1. After a minute, close CPUSTRES64 and File Explorer.
2. Switch to **Performance Monitor**.
3. In the navigation pane, right-click or access the context menu for **SEA-ADM1 Performance**, and then select **Stop**.
4. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, expand **SEA-ADM1 Performance**, select **SEA-ADM1\_DateTime-000002**, and then review the report data.
5. On the menu bar, select **Change graph type** or press Ctrl+G, and then select **Report**.
6. Record the following values:
   * **Memory/sec**
   * **Network InterfaceTotal/sec**
   * **PhysicalDisk% Disk Time**
   * **PhysicalDisk. Disk Queue Length**
   * **Processor% Processor Time**
   * **SystemQueue Length**

**Question**: Compared with your previous report, which values have changed?

**Answer**: Memory and disk activity are reduced, but processor activity has increased significantly.

**Question**: What would you recommend?

**Answer**: You should continue to monitor the server to ensure that the processor workload doesn't reach capacity.

### Results

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

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

#### Task 1: Configure subscription prerequisites

1. On **SEA-ADM1**, switch to the command prompt.
2. At the command prompt, enter the following command, and then select Enter:

* winrm quickconfig

1. You can observe that the WinRM service is already running and that it's set up for remote management.
2. On the taskbar, select **Server Manager**.
3. In **Server Manager**, select **Tools** on the toolbar, and then select **Computer Management**.
4. In **Computer Management (Local)**, expand **System Tools**, expand **Local Users and Groups**, and then select **Groups**.
5. In the results pane, double-click or select **Event Log Readers**, and then select Enter.
6. Select **Add**, and then in the **Select Users, Computers, Service Accounts or Groups** dialog box, select **Object Types**.
7. In the **Object Types** dialog box, select the **Computers** check box, and then select **OK**.
8. In the **Select Users, Computers, Service Accounts or Groups** dialog box, enter **SEA-CL1** in the **Enter the object names to select** box, and then select **OK**.
9. In the **Event Log Readers Properties** dialog box, select **OK**.
10. Switch to **SEA-CL1**.
11. Open a **Command Prompt** window, enter the following command at the command prompt, and then select Enter:

* Wecutil qc

1. Enter **Y** when prompted, and then select Enter.

#### Task 2: Create a subscription

1. Select **Start**, and then enter **Event** on the **Start** page.
2. In the **Best match** list, select **Event Viewer**.
3. In **Event Viewer**, select **Subscriptions** in the navigation pane.
4. Right-click or access the context menu for **Subscriptions**, and then select **Create Subscription**.
5. In the **Subscription Properties** dialog box, enter **SEA-ADM1 Events** in the **Subscription name** box.
6. Select **Collector initiated**, and then select **Select Computers**.
7. In the **Computers** dialog box, select **Add Domain Computers**.
8. In the **Select Computer** dialog box, enter **SEA-ADM1** in the **Enter the object name to select** box, and then select **OK**.
9. In the **Computers** dialog box, select **OK**.
10. In the **Subscription Properties – SEA-ADM1 Events** dialog box, select **Select Events**.
11. In the **Query Filter** dialog box, select the **Critical**, **Warning**, **Information**, **Verbose**, and **Error** check boxes.
12. In the **Logged** drop-down list, select **Last 7 days**.
13. In the **Event logs** drop-down list, expand **Applications and Services Logs**, expand **Microsoft**, expand **Windows**, expand **Diagnosis-PLA**, and then select the **Operational** check box.
14. In the **Query Filter** dialog box, select **OK**.
15. In the **Subscription Properties – SEA-ADM1 Events** dialog box, select **OK**.

#### Task 3: Configure a performance counter alert

1. Switch to **SEA-ADM1**.
2. In **Performance Monitor**, expand **Data Collector Sets** in the navigation pane, and then select **User Defined**.
3. Right-click or access the context menu for **User Defined**, select **New**, and then select **Data Collector Set**.
4. In the **Create new Data Collector Set Wizard**, enter **SEA-ADM1 Alert** in the **Name** box.
5. Select **Create manually (Advanced)**, and then select **Next**.
6. On the **What type of data do you want to include?** page, select **Performance Counter Alert**, and then select **Next**.
7. On the **Which performance counters would you like to monitor?** page, select **Add**.
8. In the **Available counters** list, expand **Processor**, select **% Processor Time**, select **Add**, and then select **OK**.
9. On the **Which performance counters would you like to monitor?** page, in the **Alert when** list, select **Above**.
10. In the **Limit** box, enter **10**, and then select **Next**.
11. On the **Create the data collector set?** page, select **Finish**.
12. In the navigation pane, expand the **User Defined** node, and then select **SEA-ADM1 Alert**.
13. In the results pane, right-click or access the context menu for **DataCollector01**, and then select **Properties**.
14. In the **DataCollector01 Properties** dialog box, enter **1** in the **Sample interval** box, and then select the **Alert Action** tab.
15. Select the **Log an entry in the application event log** check box, and then select **OK**.
16. In the navigation pane, right-click or access the context menu for **SEA-ADM1 Alert**, and then select **Start**.

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

1. On **SEA-ADM1**, open File Explorer.
2. Browse to **C:11**.
3. Double-click or select **CPUSTRES64.EXE**, and then select Enter.
4. In the **CPU Stress - Sysinternals: www.sysinternals.com** dialog box, right-click or access the context menu for the highlighted thread at the top of the list of running threads, select **Activity Level**, and then select **Busy (75%)**.
5. After a minute, close CPUSTRES64 and File Explorer.

#### Task 5: Verify the results

1. Switch to **SEA-CL1**.
2. In **Event Viewer**, expand **Windows Logs** in the navigation pane.
3. Select **Forwarded Events**.

**Question**: Are there any performance-related alerts?

**Answer**: Answers might vary, but there should be some events that relate to the workload imposed on **SEA-ADM1**. Events will 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.