55341

Lab 12B: Monitoring and troubleshooting Windows Server 2016

Scenario

Adatum is a global engineering and manufacturing company with its head office in London, United Kingdom. An IT office and datacenter are in London to support the London office and other locations. Adatum recently deployed a Windows Server 2016 server and client infrastructure. Because the organization has deployed new servers, it is important to establish a performance baseline with a typical load for these new servers. You have been asked to work on this project. Additionally, to make the process of monitoring and troubleshooting easier, you decide to perform centralized monitoring of event logs.

Exercise 1: Establishing a performance baseline

**Scenario**

In this exercise, you will use Performance Monitor on the server, and create a baseline by using typical performance counters.   The main tasks for this exercise are as follows:

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

Task 1: Create and start a data collector set

1. Switch to [**LON-SVR1**](urn:gd:lg:a:select-vm) and send the [**CTRL+ALT+DEL**](urn:gd:lg:a:send-vm-key-combo) command and login as [**Adatum\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. Click the **Search** button, type [**Performance**](urn:gd:lg:a:send-vm-keys) in the **Search Windows** text box, and then in the **Best match** list, click **Performance Monitor**.
3. In Performance Monitor, in the navigation pane, expand **Data Collector Sets**, and then click **User Defined**.
4. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
5. In the **Create new Data Collector Set** wizard, in the **Name** box, type [**LON-SVR1 Performance**](urn:gd:lg:a:send-vm-keys).
6. Click **Create manually (Advanced)**, and then click **Next**.
7. On the **What type of data do you want to include?** page, select the **Performance counter** check box, and then click **Next**.
8. On the **Which performance counters would you like to log?** page, click **Add**.
9. In the **Available counters** list, expand **Processor**, click **%Processor Time**, and then click **Add**.
10. In the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add**.
11. In the **Available counters** list, expand **PhysicalDisk**, click **%Disk Time**, and then click **Add**.
12. Also, undder **PhysicalDisk**, click **Avg. Disk Queue Length**, and then click **Add**.
13. In the **Available counters** list, expand **System**, click **Processor Queue Length**, and then click **Add**.
14. In the **Available counters** list, expand **Network Interface**, click **Bytes Total/sec**, click **Add**, and then click **OK**.
15. On the **Which performance counters would you like to log?** page, in the **Sample interval** text box, type [**1**](urn:gd:lg:a:send-vm-keys), and then click **Next**.
16. On the **Where would you like the data to be saved?** page, click **Next**.
17. On the **Create the data collector set?** page, click **Save and close**, and then click **Finish**.
18. In Performance Monitor, in the **Results** pane, right-click **LON-SVR1 Performance**, and then click **Start**.

Task 2: Create a typical workload on the server

1. Click **Start**, and then click **Windows PowerShell**.
2. At the command prompt, type the following command, and then press Enter:
3. Fsutil file createnew bigfile 104857600
4. At the command prompt, type the following command, and then press Enter:
5. Copy bigfile \\LON-dc1\c$
6. At the command prompt, type the following command, and then press Enter:
7. Copy \\LON-dc1\c$\bigfile bigfile2
8. At the command prompt, type the following command, and then press Enter:
9. Del bigfile\*.\*
10. At the command prompt, type the following command, and then press Enter:
11. Del \\LON-dc1\c$\bigfile\*.\*
12. Do not close the **Windows PowerShell** window.

Task 3: Analyze the collected data

1. Switch to **Performance Monitor**.
2. In the navigation pane, right-click **LON-SVR1 Performance**, and then click **Stop**.
3. In Performance Monitor, in the navigation pane, expand **Reports**, expand **User Defined**, expand **LON-SVR1 Performance**, and then click **LON-SVR1\_DateTime-000001**.
4. On the toolbar, on the **Change graph type** icon, click the drop-down arrow, click **Report**, and then review the report data.
5. Record the values that the report lists for later analysis. Recorded values include:
   * **Memory, Pages/sec**
   * **Network Interface, Bytes Total/sec**
   * **PhysicalDisk, %Disk Time**
   * **PhysicalDisk, Avg. Disk Queue Length**
   * **Processor, %Processor Time**
   * **System, Processor Queue 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 will 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 as follows:

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

Task 1: Capture performance data by using a data collector set

1. In Performance Monitor, go to **Data Collector Sets\User Defined**, and then in the results pane, start the **LON-SVR1 Performance** data collector set.

Task 2: Create additional workload on the server

1. On [**LON-SVR1**](urn:gd:lg:a:select-vm), click **Start**, and then click **Windows PowerShell ISE**.
2. In Windows PowerShell ISE, click the **Open** button, and then open the following script: **D:\Labfiles\Mod12\StressTest.ps1**
3. In Windows PowerShell ISE, click the **Run Script (F5)** button.
4. Wait until the script has finished running, and then close Windows PowerShell ISE.

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

1. Switch to **Performance Monitor**.
2. In the navigation pane, right-click **LON-SVR1 Performance**, and then click **Stop**.
3. In Performance Monitor, in the navigation pane, expand **Reports**, expand **User Defined**, expand **LON-SVR1 Performance**, and then click **LON-SVR1\_DateTime-000002**.
4. On the toolbar, on the **Change graph type** icon, click the drop-down arrow, click **Report**, and then review the report data.
   * Record the following values:
     + **Memory, Pages/sec**
     + **Network Interface, Bytes Total/sec**
     + **PhysicalDisk, %Disk Time**
     + **PhysicalDisk, Avg. Disk Queue Length**
     + **Processor, %Processor Time**
     + **System, Processor Queue Length**

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

**Answer:** Memory and disk activity are lower, 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 does not 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

**Scenario**

In this exercise, you will use LON-DC1 to collect event logs from LON-SVR1. Specifically, you will use this process to gather performance-related alerts from your network servers.

The main tasks for this exercise are as follows:

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 course completion.

Task 1: Configure subscription prerequisites

1. On [**LON-DC1**](urn:gd:lg:a:select-vm), send the [**CTRL+ALT+DEL**](urn:gd:lg:a:send-vm-key-combo) command then login in as [**Adatum\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) using password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. Click the **Search** button, in the **Search Windows** text box, type [**cmd**](urn:gd:lg:a:send-vm-keys), and then press Enter.
3. At the command prompt, type the following command, and then press Enter:
4. winrm quickconfig

**Note:** If prompted, type **Y**, and then press Enter.

1. Click the **Start** icon, then select **Server Manager**. On **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** console, in the navigation pane, expand **Adatum.com**, and then click **Builtin**.
3. In the results pane, double-click **Administrators**.
4. In the **Administrators Properties** dialog box, click the **Members** tab.
5. Click **Add**, and then in the **Select Users**, **Contacts**, **Computers**, **Service Accounts, or Groups** dialog box, click **Object Types**.
6. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
7. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** box, type [**LON-SVR1**](urn:gd:lg:a:send-vm-keys), and then click **OK**.
8. In the **Administrators Properties** dialog box, click **OK**.
9. Switch to [**LON-SVR1**](urn:gd:lg:a:select-vm).
10. Click the **Search** button, in the **Search Windows** text box, type [**Cmd**](urn:gd:lg:a:send-vm-keys), and then press Enter.
11. At the command prompt, type the following command, and then press Enter:
12. Wecutil qc
13. When prompted, type [**Y**](urn:gd:lg:a:send-vm-keys), and then press Enter.

Task 2: Create a subscription

1. On [**LON-SVR1**](urn:gd:lg:a:select-vm), click the **Search** button, type [**Event Viewer**](urn:gd:lg:a:send-vm-keys), and then press Enter.
2. In Event Viewer, in the navigation pane, click **Subscriptions**.
3. Right-click **Subscriptions**, and then click **Create Subscription**.
4. In the **Event Viewer** pop-up window, select **Yes** to start the service.
5. In the **Subscription Properties** dialog box, in the **Subscription name** text box, type [**LON-DC1 Events**](urn:gd:lg:a:send-vm-keys).
6. Click **Collector initiated**, and then click **Select Computers**.
7. In the **Computers** dialog box, click **Add Domain Computers**.
8. In the **Select Computer** dialog box, in the **Enter the object name to select** text box, type [**LON-DC1**](urn:gd:lg:a:send-vm-keys), and then click **OK**.
9. In the **Computers** dialog box, click **OK**.
10. In the **Subscription Properties - LON-DC1 Events** dialog box, click **Select Events**.
11. In the **Query Filter** dialog box, in the **Logged** drop-down list, click **Last 7 days**.
12. Select the **Critical**, **Warning**, **Information**, **Verbose**, and **Error** check boxes.
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. Switch to the **Query Filter** dialog box, and then click **OK**.
15. In the **Subscription Properties - LON-DC1 Events** dialog box, click **OK**.

Task 3: Configure a performance counter alert

1. Switch to the [**LON-DC1**](urn:gd:lg:a:select-vm) VM.
2. Open **Performance Monitor**.
3. In Performance Monitor, in the navigation pane, expand **Data Collector Sets**, and then click **User Defined**.
4. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
5. In the **Create new Data Collector Set** wizard, in the **Name** text box, type [**LON-DC1 Alert**](urn:gd:lg:a:send-vm-keys).
6. Click **Create manually (Advanced)**, and then click **Next**.
7. On the **What type of data do you want to include?** page, click **Performance Counter Alert**, and then click **Next**.
8. On the **Which performance counters would you like to monitor?** page, click **Add**.
9. In the **Available counters** list, expand **Processor**, click **%Processor Time**, click **Add**, and then click **OK**.
10. On the **Which performance counters would you like to monitor?** page, in the **Alert when list**, click **Above**.
11. In the **Limit** text box, type [**10**](urn:gd:lg:a:send-vm-keys), and then click **Next**.
12. On the **Create the data collector set?** page, click **Finish**.
13. In the navigation pane, expand the **User Defined** node, and then click **LON-DC1 Alert**.
14. In the **results** pane, right-click **DataCollector01**, and then click **Properties**.
15. In the **DataCollector01 Properties** dialog box, in the **Sample interval** text box, type [**1**](urn:gd:lg:a:send-vm-keys), and then click the **Alert Action** tab.
16. Select the **Log an entry in the application event log** check box, and then click **OK**.
17. In the navigation pane, right-click **LON-DC1 Alert**, and then click **Start**.

Task 4: Introduce additional workload on the server

1. On [**LON-DC1**](urn:gd:lg:a:select-vm), click **Start**, and then click **Windows PowerShell ISE**.
2. In Windows PowerShell ISE, click the **Open** button, and then open the following script: **D:\Labfiles\Mod12\StressTest.ps1**
3. In Windows PowerShell ISE, click the **Run Script (F5)** button.
4. Wait until the script has finished running.
5. Close Windows PowerShell ISE.

Task 5: Verify the results

1. Switch to [**LON-SVR1**](urn:gd:lg:a:select-vm).
2. In Event Viewer, in the navigation pane, expand **Windows Logs**.
3. Click **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 **LON-DC1**. Events will have an ID of 2031. If you do not receive any events, proceed with the rest of the lab. This can occur when the VM is not overloaded with the stress tool that is run.

**Results**: At the end of this exercise, you should have successfully centralized event logs and examined these logs for performance-related events.

**Congratulations!** You have now completed this course. To end the course, click End Lab in the Tools Menu. If you wish to contiue with this lab at a later date ensure you save the lab environment rather than ending it.