**The lecture 12**

[Azure Monitor](https://docs.microsoft.com/en-gb/azure/azure-monitor/overview) can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation. Installing the Log Analytics VM extension for [Windows](https://docs.microsoft.com/en-gb/azure/virtual-machines/extensions/oms-windows) and [Linux](https://docs.microsoft.com/en-gb/azure/virtual-machines/extensions/oms-linux) allows Azure Monitor to collect data from your Azure VMs. This quickstart shows you how to configure and collect data from your Azure Linux or Windows VMs using the VM extension with a few easy steps. This quickstart assumes you have an existing Azure virtual machine. If not you can [create a Windows VM](https://docs.microsoft.com/en-gb/azure/virtual-machines/windows/quick-create-portal) or [create a Linux VM](https://docs.microsoft.com/en-gb/azure/virtual-machines/linux/quick-create-cli) following our VM quickstarts.

## Sign in to Azure portal

Sign in to the Azure portal at <https://portal.azure.com>.

## Create a workspace

1. In the Azure portal, select **All services**. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics workspaces**.



1. Select **Create**, and then select choices for the following items:
	* Provide a name for the new **Log Analytics workspace**, such as DefaultLAWorkspace.
	* Select a **Subscription** to link to by selecting from the drop-down list if the default selected is not appropriate.
	* For **Resource Group**, select an existing resource group that contains one or more Azure virtual machines.
	* Select the **Location** your VMs are deployed to. For additional information, see which [regions Log Analytics is available in](https://azure.microsoft.com/regions/services/).
	* If you are creating a workspace in a new subscription created after April 2, 2018, it will automatically use the Per GB pricing plan and the option to select a pricing tier will not be available. If you are creating a workspace for an existing subscription created before April 2, or to subscription that was tied to an existing EA enrollment, select your preferred pricing tier. For additional information about the particular tiers, see [Log Analytics Pricing Details](https://azure.microsoft.com/pricing/details/log-analytics/).



1. After providing the required information on the **Log Analytics workspace** pane, select **OK**.

While the information is verified and the workspace is created, you can track its progress under **Notifications** from the menu.

## Enable the Log Analytics VM Extension

For Windows and Linux virtual machines already deployed in Azure, you install the Log Analytics agent with the Log Analytics VM Extension. Using the extension simplifies the installation process and automatically configures the agent to send data to the Log Analytics workspace that you specify. The agent is also upgraded automatically when a newer version is released, ensuring that you have the latest features and fixes. Before proceeding, verify the VM is running otherwise the process will fail to complete successfully.

1. In the Azure portal, select **All services** found in the upper left-hand corner. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics workspaces**.
2. In your list of Log Analytics workspaces, select DefaultLAWorkspace created earlier.
3. On the left-hand menu, under Workspace Data Sources, select **Virtual machines**.
4. In the list of **Virtual machines**, select a virtual machine you want to install the agent on. Notice that the **Log Analytics connection status** for the VM indicates that it is **Not connected**.
5. In the details for your virtual machine, select **Connect**. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the **Status** shows **Connecting**.
6. After you install and connect the agent, the **Log Analytics connection status** will be updated with **This workspace**.

## Collect event and performance data

Azure Monitor can collect events from the Windows event logs or Linux Syslog and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows system log and Linux Syslog, and several common performance counters to start with.

### Data collection from Windows VM

1. Select **Advanced settings**.



1. Select **Data**, and then select **Windows Event Logs**.
2. You add an event log by typing in the name of the log. Type **System** and then select the plus sign **+**.
3. In the table, check the severities **Error** and **Warning**.
4. Select **Save** at the top of the page to save the configuration.
5. Select **Windows Performance Data** to enable collection of performance counters on a Windows computer.
6. When you first configure Windows Performance counters for a new Log Analytics workspace, you are given the option to quickly create several common counters. They are listed with a checkbox next to each.



Select **Add the selected performance counters**. They are added and preset with a ten second collection sample interval.

1. Select **Save** at the top of the page to save the configuration.

### Data collection from Linux VM

1. Select **Syslog**.
2. You add an event log by typing in the name of the log. Type **Syslog** and then select the plus sign **+**.
3. In the table, deselect the severities **Info**, **Notice** and **Debug**.
4. Select **Save** at the top of the page to save the configuration.
5. Select **Linux Performance Data** to enable collection of performance counters on a Linux computer.
6. When you first configure Linux Performance counters for a new Log Analytics workspace, you are given the option to quickly create several common counters. They are listed with a checkbox next to each.



Select **Apply below configuration to to my machines** and then select **Add the selected performance counters**. They are added and preset with a ten second collection sample interval.

1. Select **Save** at the top of the page to save the configuration.

## View data collected

Now that you have enabled data collection, lets run a simple log search example to see some data from the target VMs.

1. In the selected workspace, from the left-hand pane, select **Logs**.
2. On the Logs query page, type Perf in the query editor and select **Run**.



For example, the query in the following image returned 10,000 performance records. Your results will be significantly less.



## Clean up resources

When no longer needed, delete the Log Analytics workspace. To do so, select the Log Analytics workspace you created earlier and on the resource page select **Delete**.

