Manage the Event Log with the command line

For many of us, using the command line - Command Line to control and use some of the functions in the Windows system will cause them to have headaches and problems. However, if you have to set up an automatic function system in Windows and other server operating systems, the Command Line is an irreplaceable tool ...

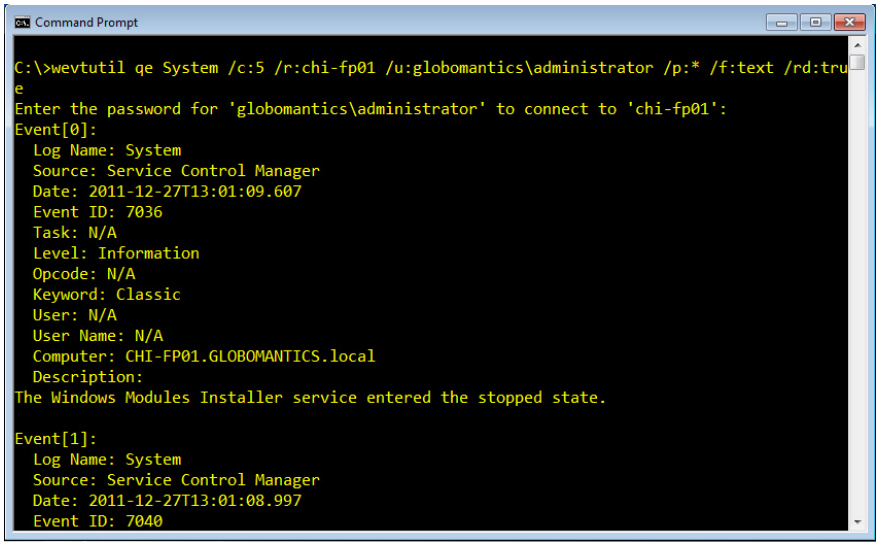
In the following article, we will show you some of the functions in **Windows 7 Desktop** that can be done and controlled easily by the command line.

Manage Event Log:

First, open the **Command Prompt** (**Start> Run>** type **cmd** and press **Enter**) and find out about the utility **WEVTUTIL.EXE**

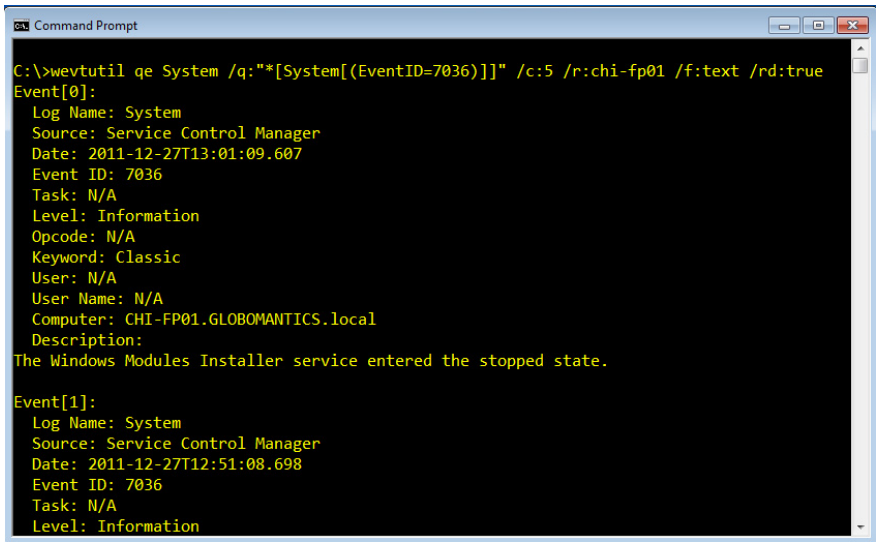
C:> wevtutil /?
Windows Events Command Line Utility.Enables you to retrieve information about event logs and publishers, install
and uninstall events manifests, run queries, and export, archive, and clear logs.Usage:B?n có th? s? d?ng nh? d?? i (cho example, ep / uni) or long (for example,
enum-publishers / unicode) version of the command and options names. Commands,
các tùy ch?n và tùy ch?n tùy ch?n không có tùy ch?n-sensitive.
.

The initial default feature of this statement is to query directly to the log files on the local computer, if you want to apply it to the remote computer - the remote control, then add the / r parameter. However, we can only execute this query on a single computer at a time only. The basic syntax of **WEVTUTIL** is in the form of:*C:> wevtutil qe*The following table are frequently used parameters:When you connect to the remote computer, the system will use the identity information of the current account, but if you want to change, you use the syntax as below:*/ u: domainusername and / p:*When pairing this information together, suppose that you want to gather information about the 5 components in the **System Event Log** on the computer **CHI-FP01:***C:> wevtutil qe System / c: 5 / r: chi-fp01 / u: globomanticsadministrator / p: * / f: text / rd: true*In fact, we should not type the password as text here, but rather use the * character as shown below:



However, it is not easy to find and understand the component information in the log file log, because **Windows Event Log** requires users to have knowledge of XML. If you want a specific record, you need to use the **/ q** parameter, which requires an XPath. For experienced users it is recommended to use the syntax form as follows: *"/ q: * [[(* xmlvalue=value> *)]] "*The **XML** value section here is the **XML node** name, select that component to check:
C:> wevtutil qe System / c: 1700104110100x20000000000000013218SystemCLIENT1.jdhlab.local1S-1-5-21-3957442467-353870018-3926547339-500

Assuming that we want to execute a query to **EventID 7036** , we will use the following command:*C:> wevtutil qe System / q: "* [System [(EventID = 7036)]]" / c: 5 / r: chi-fp01 / f: text / rd: true*And the results show up at this step:



In addition, another frequently used function here is to collect information about components and related information, such as **Error** or **Warning** . We can do it, but it must be based on the corresponding **Level** :**Level Description** Level 1CriticalLevel 2ErrorLevel 3WarningLevel 4InformationTherefore, to get information about the 5 most recent errors in the **System Event Log** of **CHI-DC01** , type the command:*C:> wevtutil qe system "/ q: * [System [(Level = 2)]]" / f: text / c: 5 / rd: True / r: chi-dc01 | more*Or switch to text format with the conversion command:*C:> wevtutil qe system "/ q: * [System [(Level = 2)]]" / f: text / c: 5 / rd: True / r: chi-dc01> d: dc01-system-err.txt*Or make the order more complicated:*C:> wevtutil qe system "/ q: * [System [(Level = 2 or Level = 3)]]" / f: text / c: 5 / rd: True / r: chi-dc01 | more*But you need to be careful, because uppercase

and lowercase letters here must be absolutely accurate.

Advanced Query command with Event Viewer Management Console:

For complex query statements, we should open the **Event Viewer Management** function and use the graphical interface to create the query. Then, look at the XML file and save the necessary piece of information into the **Command Line** . For frequently used components, you should save it as a text file, then enter it into the query. Examples are as follows:Copy and save the above code into a text file, then we can use the query with the **Command Line:***C:> wevtutil qe s: scmquery.txt / sq: true / c: 5 / f: text / r: chi-fp01*Instead of the log file name, we explicitly specify the path to the **XML** query statement and set the parameter **/ sq** to **True** . If there are no matching events, the system will not return any suitable data. In the next section of the article, we will discuss more about how to manage the **Event Log** . Good luck!