

Script to search event viewer log

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.scripting/2005-09/msg00007.html>

- *From:* "Marco Shaw" <marco@xxxxxxxxxxxxx>
 - *Date:* Wed, 31 Aug 2005 15:22:35 -0300
-

Windows 2000

I need to write a script that will search the Windows Event Log for all events with source XYZ that occurred in the last 15 minutes or so, take each event and make the details of the source, computer name, and message details/description available for some further scripting.

WMI is pretty powerful at being able to do this, but I have not been able to figure out how to get the start time and end times setup.

I had put together something like this which I had somewhat working for Win2k3, but WbemScripting.SWbemDateTime isn't available with Windows 2000:

```
Const CONVERT_TO_LOCAL_TIME = True

Set dtmStartDate = CreateObject("WbemScripting.SWbemDateTime")
Set dtmEndDate = CreateObject("WbemScripting.SWbemDateTime")
DateToCheckAgo = DateAdd("n",-15,Now())
DateToCheckAgo = DateAdd("h",-3,DateToCheckAgo)
DateToCheck = CDate(Now())
DateToCheck = DateAdd("h",-3,DateToCheck)
dtmStartDate.SetVarDate DateToCheckAgo, CONVERT_TO_LOCAL_TIME
dtmEndDate.SetVarDate DateToCheck, CONVERT_TO_LOCAL_TIME

Wscript.Echo DateToCheckAgo
Wscript.Echo DateToCheck
Wscript.Echo dtmStartDate
Wscript.Echo dtmEndDate
Wscript.Echo ""

strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")
Set colEvents = objWMIService.ExecQuery _
("Select * from Win32_NTLogEvent Where TimeWritten >= " & dtmStartDate
& " and TimeWritten < " & dtmEndDate & " and SourceName = 'VBRuntime'")

For Each objEvent in colEvents
```

Script to search event viewer log

```
Wscript.Echo "Category: " & objEvent.Category
Wscript.Echo "Computer Name: " & objEvent.ComputerName
Wscript.Echo "Event Code: " & objEvent.EventCode
Wscript.Echo "Source Name: " & objEvent.SourceName
Wscript.Echo "Message: " & objEvent.Message
'strMessage = objEvent.Message
Wscript.Echo "Record Number: " & objEvent.RecordNumber
Wscript.Echo "Source Name: " & objEvent.SourceName
Wscript.Echo "Time Written: " & objEvent.TimeWritten
Wscript.Echo "Event Type: " & objEvent.Type
Wscript.Echo "User: " & objEvent.User
Wscript.Echo objEvent.LogFile
Wscript.Echo ""

SNMPTrap objEvent.SourceName,objEvent.ComputerName,objEvent.Message
Next

Sub SNMPTrap (strMessage1,strMessage2,strMessage3)

Set obj_TrapGen = CreateObject("ComTrapGen.NctComTrapGen")

' Setup parameters

' Destination IP address
obj_TrapGen.DestinationIP="111.111.111.111"

' Destination port
obj_TrapGen.DestinationPort="162"

' Community name
obj_TrapGen.Community="private"

' Sender IP address
obj_TrapGen.SendersIP="222.222.222.222"

' Senders OID
obj_TrapGen.SendersOID="1.3.6.1.4.1.2854.6.1.2.1"

' Generic Type
obj_TrapGen.GenericType="6"

' Specific Type
obj_TrapGen.SpecificType="1"

' Add variable bindings...

' Add a variable binding, of the type STRING
Call obj_TrapGen.AddStringVarbind("1.3.6.1.4.1.2854.6.1.2.1.1",
strMessage1)

' Add a variable binding, of the type STRING
```

Script to search event viewer log

```
Call obj_TrapGen.AddStringVarbind("1.3.6.1.4.1.2854.6.1.2.1.2",  
strMessage2)
```

```
' Add a variable binding, of the type STRING
```

```
Call obj_TrapGen.AddStringVarbind("1.3.6.1.4.1.2854.6.1.2.1.3",  
strMessage3)
```

```
' Send a SNMP version 1 trap
```

```
obj_TrapGen.SendV1Trap()
```

```
End Sub
```

```
Set dtmStartDate = Nothing
```

```
Set dtmEndDate = Nothing
```

```
Set objWMIService = Nothing
```

```
Set colEvents = Nothing
```

```
Set obj_TrapGen = Nothing
```

```
Wscript.Quit
```

How can I get this working with VBScript and or WMI?

Marco

.

- ***Follow-Ups:***

- ◆ ***Re: Script to search event viewer log***

- ◆ *From:* Dominic Johnson

- Prev by Date: ***RE: Error handling in a Do Loop***
- Next by Date: ***VBScript to delete profile remotly***
- Previous by thread: ***RE: Error handling in a Do Loop***
- Next by thread: ***Re: Script to search event viewer log***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***