

Content of WMI MSNT_SystemTrace Query.vbs (Site 1)

On Error Resume Next

```
Const wbemFlagReturnImmediately = &h10
Const wbemFlagForwardOnly = &h20
```

```
arrComputers = Array(".')
```

```
For Each strComputer In arrComputers
```

```
    WScript.Echo
```

```
    WScript.Echo "=====
```

```
    WScript.Echo "Computer: " & strComputer
```

```
    WScript.Echo "=====
```

```
    Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\WMI")
```

```
    Set collItems = objWMIService.ExecQuery("SELECT * FROM MSNT_SystemTrace", "WQL", _
        wbemFlagReturnImmediately + wbemFlagForwardOnly)
```

```
    For Each objItem In collItems
```

```
        strEventGuid = Join(objItem.EventGuid, ",")
```

```
        WScript.Echo "EventGuid: " & strEventGuid
```

```
        WScript.Echo "EventSize: " & objItem.EventSize
```

```
        WScript.Echo "EventType: " & objItem.EventType
```

```
        WScript.Echo "Flags: " & objItem.Flags
```

```
        WScript.Echo "Instancelid: " & objItem.Instancelid
```

```
        WScript.Echo "KernelTime: " & objItem.KernelTime
```

```
        WScript.Echo "MofData: " & objItem.MofData
```

```
        WScript.Echo "MofLength: " & objItem.MofLength
```

```
        strParentGuid = Join(objItem.ParentGuid, ",")
```

```
        WScript.Echo "ParentGuid: " & strParentGuid
```

```
        WScript.Echo "ParentInstancelid: " & objItem.ParentInstancelid
```

```
        WScript.Echo "ReservedHeaderField: " & objItem.ReservedHeaderField
```

```
        WScript.Echo "ThreadId: " & objItem.ThreadId
```

```
        WScript.Echo "TimeStamp: " & objItem.TimeStamp
```

```
        WScript.Echo "TraceLevel: " & objItem.TraceLevel
```

```
        WScript.Echo "TraceVersion: " & objItem.TraceVersion
```

```
        WScript.Echo "UserTime: " & objItem.UserTime
```

```
        WScript.Echo
```

```
    Next
```

```
Next
```