

Re: Is there a way to query Security Event Log with Filter in C#?

Re: Is there a way to query Security Event Log with Filter in C#?

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.csharp/2007-01/msg00769.html>

- *From:* Pucca <Pucca@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 5 Jan 2007 14:16:00 -0800
-

Thanks Willy. I am login as an administrator on my Win2k server. Is there any other setting that I need to configure for an administrator? Thanks.

—

Thanks.

"Willy Denoyette [MVP]" wrote:

"Pucca" <Pucca@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:781462FF-AAFB-4197-9942-3FE17C6CDF23@xxxxxxxxxxxxxxxxxxxx>

The odd thing is that it works when I change the logfile = 'Application'.
Wieht Security it retrieves 0 entry. Why is that so? I did verify that I
have over 55k of entries in Security log in Event Viewer.

—

Thanks.

"Pucca" wrote:

Thanks Peter. I tried it in my code but it's just exiting when it
eaches the
statement mos.get(). Can you see what's wrong here? Also,
where can I look
up syntax format and the properties names for the Security
log? Thanks.

```
private void GetLog()
{
//string SomeDateTime = "20060101000000.000000+000";
//string Query = String.Format("SELECT * FROM
Win32_NTLogEvent WHERE
Logfile = 'Security' AND TimeGenerated > '{0}'",
```

Re: Is there a way to query Security Event Log with Filter in C#?

```
SomeDateTime);
string Query = String.Format("SELECT * FROM
Win32_NTLogEvent WHERE
Logfile = 'Security'");

object o;
string name;
try
{
ManagementObjectSearcher mos = new
ManagementObjectSearcher(Query);
foreach (ManagementObject mo in mos.Get())
{
foreach (PropertyData pd in mo.Properties)
{
o = mo[pd.Name];
if (o != null)
{

//Console.WriteLine(String.Format("{0}: {1}", pd.Name,
mo[pd.Name].ToString()));
}
}
}
mos.Dispose();
}
catch (Exception e)
{
MessageBox.Show(e.Message);
}

}
--
Thanks.
```

"Petar Repac" wrote:

Hi !

You can try WMI query for this.
Example that filters event log by LogFile
and TimeGenerated.

```
using System;
using System.Collections.Generic;
using System.Text;
using System.Management;
```

Re: Is there a way to query Security Event Log with Filter in C#?

```
namespace QueryEventLog {

class Program {
static void Main(string[] args) {
string SomeDateTime =
"20070101000000.000000+000";
string Query = String.Format("SELECT *
FROM Win32_NTLogEvent
WHERE Logfile = 'Application' AND
TimeGenerated > '{0}'", SomeDateTime);
ManagementObjectSearcher mos = new
ManagementObjectSearcher(Query);
object o;

foreach (ManagementObject mo in
mos.Get()) {

Console.WriteLine("////////////////////////////////////");
foreach (PropertyData pd in mo.Properties) {
o = mo[pd.Name];
if (o != null) {
Console.WriteLine(String.Format("{0}:
{1}", pd.Name,
mo[pd.Name].ToString()));
}
}
}

Console.ReadLine();
}
}
}
```

Hope it helps.

Petar Repac

Pucca wrote:

Thank you Jani. I'm already using the eventLog class and processing each log entry and filtering them in my C# code (vs2005, .net2.0) and then place the filtered / qualified rows in to a dataset table.

The problem is this is taking

Re: Is there a way to query Security Event Log with Filter in C#?

a long time. It's taking 45
seconds just to
read about 45k of entries(I
get the entrycollection then
use a logentry
variable to read each one).
Are there anyway to
improve this?

Only administrators can read the security log!

Willy.