

Re: Track Domain User Logons and Logoffs

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2004-06/0860.html>

From: John Saunders (johnwsaundersiii_at_notcoldmail.com)

Date: 06/03/04

Date: Thu, 3 Jun 2004 17:51:23 -0400

"Bruno Mendonça" <anonymous@discussions.microsoft.com> wrote in message news:17c0b01c4499c\$9926d000\$a301280a@phx.gbl...

> > *In Kerberos, computers are actually logging in and out,*
> > *as though they were*
> > *users. That's what those "\$" logins are. Kerberos*
> > *provides two-way*
> > *authentication, where the server can be sure who the*
> > *client is, and the*
> > *client can be sure who the server is.*
> >
> > *I believe the event log entry would more accurately*
> > *say "Principal name"*
> > *instead of "user name", as there can be other types of*
> > *principal logging in.*
> > --
> > *John Saunders*
> > *johnwsaundersiii at hotmail*
>
> *This are the properties I can access to:*
>
> *TargetInstance.Category*
> *TargetInstance.EventCode*
> *TargetInstance.EventIdentifier*
> *TargetInstance.EventType*
> *TargetInstance.RecordNumber*
> *TargetInstance.CategoryString*
> *TargetInstance.ComputerName*
> *TargetInstance.Logfile*
> *TargetInstance.Message*
> *TargetInstance.SourceName*
> *TargetInstance.Type*
> *TargetInstance.TimeGenerated*
> *TargetInstance.TimeWritten*
> *TargetInstance.User*
>
> *None of them has any additional information about the*

> user, except for the ones I'm already outputing (Message
> and User)
>
> There is also the chance of creating a Management Event on
> the Server Explorer of vb.Net and have it listen to log
> events. Once you create a NT Event Log Query and start it,
> it automatically writes the events to the Output window
> and it display additional information. So I created one
> and started it. Very quickly I logged to Computer
> Dosinsads3 under bruno_mendonca, logged of and stoped the
> event query. Maybe 20 seconds went by and from the output
> genetrated I retrieved the events refering to either
> bruno_mendonca or Dosinsads3. There where 26! For a simple
> logon and logoff. I can't tell which one refers to the
> logon and which to the logoff...
>
> Here are 3 examples:
>
> 1 –
>
> Category = 9; CategoryString = "Account Logon\n";
> ComputerName = "SEDEDC02"; EventCode = 673;
> InsertionStrings =
> {"bruno_mendonca", "CMLLOURES.PT", "DOSINSADS3\$", "%{S-1-5-
> 21-195237392-612787311-312552118-
> 5296}", "0x40810010", "0x17", "10.11.1.36"};
> Message = "Service Ticket Granted:\n\n\tUser
> Name:\t\tbruno_mendonca\n\n\tUser
> Domain:\t\tCMLLOURES.PT\n\n\tService Name:\t\tDOSINSADS3
> \$\n\n\tService ID:\t\t%{S-1-5-21-195237392-612787311-
> 312552118-5296}\n\n\tTicket Options:\t\t0x40810010
> \n\n\tTicket Encryption Type:\t0x17\n\n\tClient
> Address:\t\t10.11.1.36\n\n";
> TimeGenerated = "20040603191448.000000+060"; Type
> = "audit success"; User = "NT
> AUTHORITY\SYSTEM"; }; };
>
>
> 2 –
>
> Category = 2; CategoryString = "Logon/Logoff\n";
> ComputerName = "SEDEDC02"; EventCode = 540;
> InsertionStrings =
> {"bruno_mendonca", "CMLLOURES", "(0x0,0xEEDE5F)", "3", "Kerb
> eros", "Kerberos", ""};
> Message = "Successful Network Logon:\n\n\tUser
> Name:\tbruno_mendonca\n\n\tDomain:\tCMLLOURES\n\n\tLogon
> ID:\t\t(0x0,0xEEDE5F)\n\n\tLogon Type:\t3\n\n\tLogon
> Process:\tKerberos\n\n\tAuthentication
> Package:\tKerberos\n\n\tWorkstation Name:\t\n";
> TimeGenerated = "20040603191448.000000+060"; Type

```
> = "audit success"; User
> = "CMLOURES\\bruno_mendonca"; }; };
>
>
> 3 -
>
> Category = 2; CategoryString = "Logon/Logoff\n";
> ComputerName = "SEDEDC02"; EventCode = 540;
> InsertionStrings =
> {"bruno_mendonca", "CMLOURES", "(0x0,0xEEDE8F)", "3", "Kerb
> eros", "Kerberos", ""};
> Message = "Successful Network Logon:\n\n\tUser
> Name:\tbruno_mendonca\n\n\tDomain:\tCMLOURES\n\n\tLogon
> ID:\t(0x0,0xEEDE8F)\n\n\tLogon Type:\t3\n\n\tLogon
> Process:\tKerberos\n\n\tAuthentication
> Package:\tKerberos\n\n\tWorkstation Name:\t\n";
> TimeGenerated = "20040603191448.000000+060"; Type
> = "audit success"; User
> = "CMLOURES\\bruno_mendonca"; }; };
>
>
> The last 2 are identical!
>
> If you wish to see them all look at this 14kb .txt file:
> http://www.geocities.com/bmmpt/events.txt
>
```

If you look carefully at the last two, you'll see that they have different logon ids.

--
John Saunders
johnwsaundersiii at hotmail