source: http://www.MSSQLTips.com/tip.asp?id=3017 -- printed: 10/17/2013 12:37:51 PM

Real time auditing of failed SQL Server logins with user settable performance counters in Performance Monitor

Written By: Daniel Farina -- 8/26/2013

Problem

In some circumstances you will need to raise an alert when there are repeated SQL Server login failures. For example, let's say we need to be notified of a potential brute force attack on our SQL Servers. See how you can address this need with a User Settable Object Performance Counter in Performance Monitor.

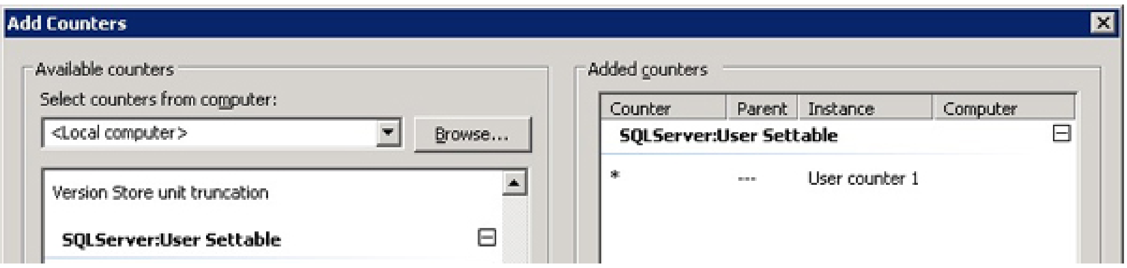
Solution

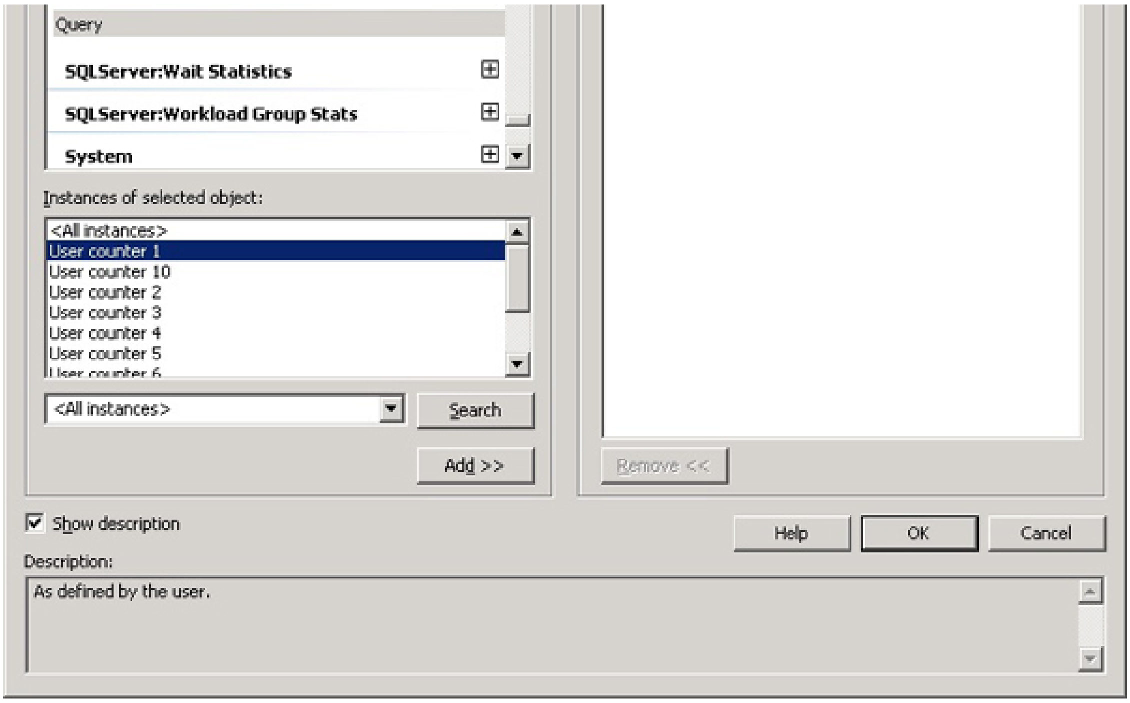
In Performance Monitor, have you ever asked yourself what are the User Settable object Performance Counters and how can I use them? In this tip, I will show you how to audit failed logins with these parameters in Performance Monitor.

User Settable Object Performance Counter in Performance Monitor

The User Settable object allows you to create custom performance counter instances. It contains 10 instances of the query counter: User counter 1 through User counter 10. These counters map to the SQL Server stored procedures **sp_user_counter1** through **sp_user_counter10**. As these stored procedures are executed by user applications, the values set by the stored procedures are displayed in System Monitor. A counter can monitor any single integer value.

Something to keep in mind is that these counters aren't automatically pooled by the OS. Instead you have to change their values by calling the **sp_user_counter#** stored procedure, where # is a number from 1 to 10.





Instances of selected object:

- <All instances>
- User counter 1
- User counter 10
- User counter 2
- User counter 3
- User counter 4
- User counter 5
- User counter 6

<All instances>

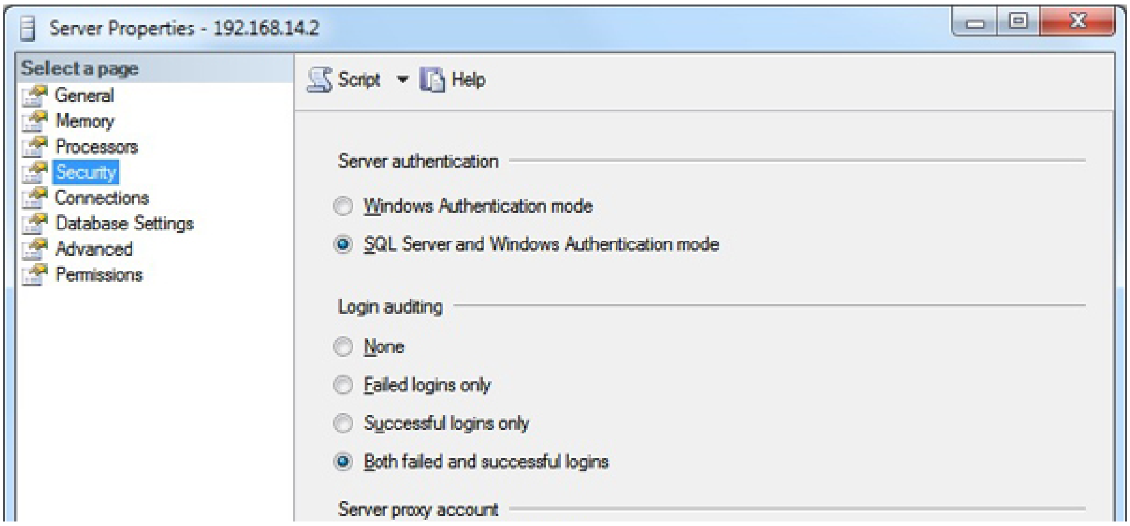
☑ Show description

Description:

As defined by the user.

Configuring SQL Server to Audit for Failed Logins

In order to audit failed logins, you have to configure login auditing in the server properties security page.



Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

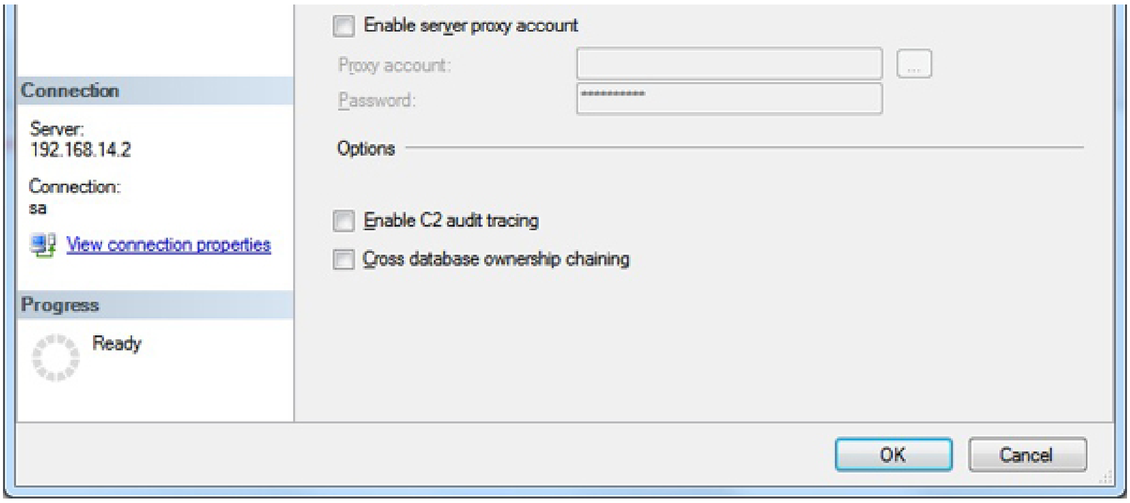
○ None

○ Failed logins only

○ Successful logins only

● Both failed and successful logins

Server proxy account



□ Enable server proxy account

Proxy account:

Password: ***********

Options

□ Enable C2 audit tracing

□ Cross database ownership chaining

Connection

Server:
192.168.14.2

Connection:
sa

Progress

Ready

Setting the counter for master.dbo.sp_user_counter1

I have created a script that sets the value of User counter 1 by calling sp_user_counter1 and passing the number of failed logins. This script only reads the current error log because its purpose is the real time monitoring of failed logins, so I think that is useless to check for historical data. But remember, SQL Server switches the error log on every service restart, so you may want to handle this issue on the script. Here is a clue: use the **sp_enumerrorlogs** system stored procedure to find the log numbers by date.

```
-- =============================================
-- Author:  Daniel Farina
-- Create date: 07/26/2013
-- Description: Reads Error log to find the number of
--  failed logins and sets sp_user_counter1 with that value.
--
-- @LogDate: Date to start search. Default NULL = No limit
-- =============================================
CREATE PROCEDURE AuditFailedLoginsUserCounter
@LogDate  DATETIME = NULL
AS
BEGIN

 SET NOCOUNT ON;

 DECLARE @FailedCount  INT

  CREATE TABLE #ErrorLog

 (
  ID    INT IDENTITY(1,1),
  LogDate   DATETIME,
  ProcessInfo  VARCHAR(50),
  TextMsg   VARCHAR(1000),
  CONSTRAINT PK1 PRIMARY KEY CLUSTERED (ID)
 )

 INSERT INTO #ErrorLog
 EXEC master.dbo.sp_readerrorlog 0, 1, 'Login failed'

 SELECT  @FailedCount = COUNT(0)
   FROM #ErrorLog
   WHERE @LogDate IS NULL OR LogDate >= @LogDate

 EXEC master.dbo.sp_user_counter1 @FailedCount

 DROP TABLE #ErrorLog
END
GO
```

Configure a SQL Server Agent Job to Monitor for Failed Logins

Remember that you have to manually update the counter value, so in order to achieve that we must create a SQL Server Agent Job that executes the stored procedure. I have configured the job to run every half hour. In order to run this script you will need to change the 'SELECT @Database = N'MyDB'' parameter to your database.

```
-- =============================================
-- Author:  Daniel Farina
-- Create date: 07/26/2013
-- Description: Create job to set User Settable Performance Counter
-- with [AuditFailedLoginsUserCounter] Stored Procedure
-- =============================================
USE [msdb]
GO

/****** Object:  Job [Failed Login Audit Performance Counter]   ******/
BEGIN TRANSACTION
DECLARE @ReturnCode INT
DECLARE @Database NVARCHAR(50)
-- SET @Database to the database in wich the stored procedure AuditFailedLoginsUserCounter is.
SELECT @Database = N'MyDB'
SELECT @ReturnCode = 0

/****** Object:  JobCategory [[Uncategorized (Local)]]]  ******/
```

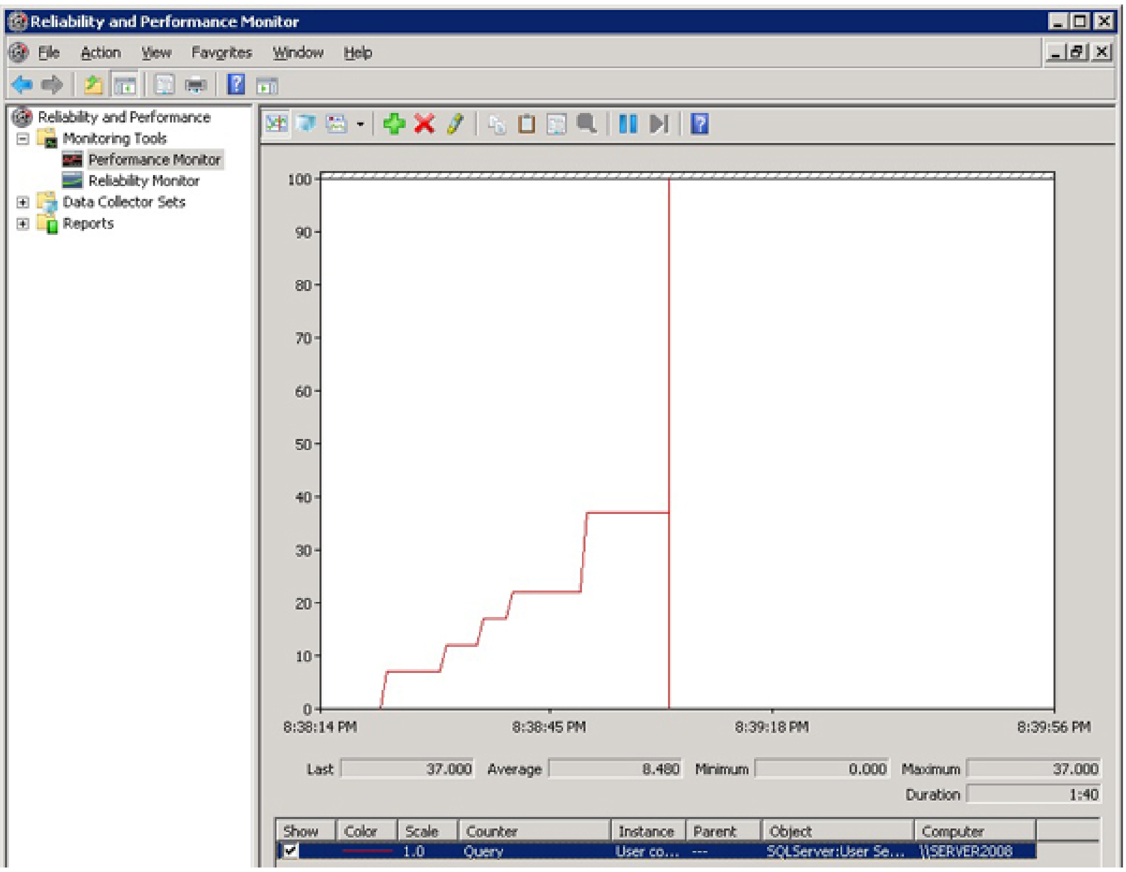
Test the SQL Server Failed Login Process

First, configure Performance Monitor to capture the data for the SQLServer:User Settable Counter 1.

Here is a test script that connects with wrong credentials to show you the counter in action. Update this script to have your development SQL Server name for the server parameter i.e. '-S SERVER2008 ' for sqlcmd. Run this code to generate data in Performance Monitor.

```
DECLARE @FailedCount INT
SET @FailedCount = 5
WHILE @FailedCount > 0
BEGIN
 EXEC master.dbo.xp_cmdshell 'sqlcmd -S SERVER2008 -U sa -P 1234' , NO_OUTPUT
 SET @FailedCount = @FailedCount - 1
END
```

And here you have a screen capture from Performance Monitor of the User Settable performance counter showing the failed logins count.



Last 37.000 Average 8.480 Minimum 0.000 Maximum 37.000
Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	1.0	Query	User co...	---	SQLServer:User Se...	\\SERVER2008

Next Steps

- Review Error log management - http://www.mssqltips.com/sqlservertip/1155/sql-server-2005-error-log-management/.
- See how to read SQL server log files with T-SQL - http://www.mssqltips.com/sqlservertip/1476/reading-the-sql-server-log-files-using-tsql/.
- Check out these cateogories of tips:
    - SQL Server Monitoring
    - SQL Server Security
- Look for other uses of the user settable performance counter.

Copyright (c) 2006-2013 Edgewood Solutions, LLC All rights reserved
privacy | disclaimer | copyright | advertise | about
authors | contribute | feedback | giveaways | user groups | whitepapers
Some names and products listed are the registered trademarks of their respective owners.