

## Re: Setup alert for failed sa login

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2003-11/0417.html>

---

**From:** Eric Sabine ([mopar41\\_at\\_hyottmail.com](mailto:mopar41_at_hyottmail.com))

**Date:** 11/26/03

Date: Wed, 26 Nov 2003 16:25:16 -0500

Here's a set of scripts that you can start with. This is not a perfect solution. In fact I have been meaning to improve it; perhaps I will start. Yukon supposedly will also track the IP address when a failed login attempt happens. Now you have to resort to profiler.

hth

Eric

Here is basically what happens. My ver also depends on you having xp\_smtp\_sendmail. Get it from <http://sqldev.net/xp/xpsmtp.htm>

0) I increased the number of SQL Server Logs from 6 to a high number. Go with whatever you want.

1) a 3-step job runs regularly.

a) first step is to cycle the error log (I reboot SQL server very infrequently, so unless I cycle, I get very big logs --> exec sp\_cycle\_errorlog

b) a step scans the most recent (but not the current) log for failed login attempts.

```
declare @phrase_to_find varchar(100)
set @phrase_to_find = 'Login failed'
```

```
declare @string varchar(200)
set @string = 'findstr /C:"' + @phrase_to_find + '" E:\MSSQL\LOG\ERRORLOG.1
> E:\MSSQL\LOG\LOG_SCANS\Scan_output.txt'
```

```
exec master.dbo.xp_cmdshell @string
```

c) A stored proc runs to email results to all SQL admins --> exec master.dbo.sp\_sendFailureLoginEmailToAdmins

Below are the sprocs.

microsoft.public.sqlserver.security: Re: Setup alert for failed sa login

```
CREATE PROC sp_checkAvailabilityOfSmtpServer (
  @server_dns NVARCHAR(100)
)
AS
DECLARE @rc int
EXEC @rc = master.dbo.xp_smtp_sendmail @server = @server_dns, @ping = 1
IF @@ERROR <> 0 RETURN -100
RETURN @rc
GO

CREATE PROC sp_sendFailureLoginEmailToAdmins
AS

/*
Stored procedure created by Eric Sabine to email login failure attempts to
SQL admins
Created 11/14/02

Returns -101 - No valid SMTP server could be contacted, net send instead
*/

SET NOCOUNT ON
CREATE TABLE #BatchResults (Result VARCHAR(500))

DECLARE @netSendMessage VARCHAR(100)
DECLARE @netSendStation VARCHAR(50)

-- Go to MSDB and get the "principal" sql admin's net send address

-- This section depends on you having created an OPERATOR called
"Principal_Admin_Workstation" where the main DBA's

-- workstation is named for the NETSEND. You can dump this if you want.
SELECT @netSendStation = netsend_address FROM msdb.dbo.sysoperators WHERE
name = 'Principal_Admin_Workstation'
SET @netSendMessage = 'net send ' + @netSendStation + ' "login failure on
SQLSERVER1, can"t relay SMTP either."'

-----

--
-- Use a quick cursor to iterate through all of the server admins. Cursors
suck, I know.
-- and concatenate their email addresses into a semicolon delimited string
DECLARE @emails NVARCHAR(200)
DECLARE @emailString NVARCHAR(200)
SET @emailString = ''
DECLARE curOperatorEmails CURSOR FOR
SELECT email_address FROM msdb.dbo.sysoperators WHERE email_address IS NOT
NULL
OPEN curOperatorEmails
FETCH NEXT FROM curOperatorEmails INTO @emails
WHILE @@FETCH_STATUS = 0
```

Re: Setup alert for failed sa login

## microsoft.public.sqlserver.security: Re: Setup alert for failed sa login

```
BEGIN
SET @emailString = @emailString + @emails + ';'
FETCH NEXT FROM curOperatorEmails INTO @emails
END
CLOSE curOperatorEmails
DEALLOCATE curOperatorEmails
-----
--
INSERT #BatchResults
EXEC master..xp_cmdshell 'dir e:\mssql\log\log_scans\'
DECLARE @size varchar(50)
SELECT @size = LTRIM(SUBSTRING(result, 19, 20)) FROM #batchresults WHERE
result LIKE '%scan_output.txt%'
IF @size <> '0'
BEGIN
-- send the email.
DECLARE @rc INT
DECLARE @email_server NVARCHAR(32)
SET @email_Server = N'myFirstSmtpServer.domain.com' -- I have access to 2
SMTP servers, so I try them both.
EXEC @rc = master.dbo.sp_checkAvailabilityOfSmtpServer @server_dns =
@email_server
IF @rc <> 0
-- We couldn't contact the primary SMTP server. Try a second one.
BEGIN
-- Change the SMTP server and test that one too
SET @email_Server = N'mySecondSmtpServer.domain.com'
EXEC @rc = master.dbo.sp_checkAvailabilityOfSmtpServer @server_dns =
@email_server
IF @rc <> 0
BEGIN
EXEC master.dbo.xp_cmdshell @netSendMessage
RETURN -101
END
END
-- We found a valid SMTP server.
BEGIN
EXEC @rc = master.dbo.xp_smtp_sendmail
@FROM = N'server@sqlserver.com',
@FROM_NAME = N'SQLServer',
@TO = @emailString,
@subject = N'Failed Login Attempt',
@attachments = N'E:\MSSQL\LOG\LOG_SCANS\Scan_output.txt',
@type = N'text/html',
@server = @email_server
IF @rc <> 0 or @@error <> 0
BEGIN
EXEC master..xp_cmdshell @netSendMessage
RETURN -102
END
END
END
RETURN 0
DROP TABLE #batchResults
SET NOCOUNT OFF
GO
"Mike" <anonymous@discussions.microsoft.com> wrote in message
news:79da01c3b45c56bfc8cd05a601280a@phx.gbl...> Is there a way to setup an
alert, or some type of
> notification method, for failed sa logins?
>
> Thank you.
```

Re: Setup alert for failed sa login