**Audit Users logging in using "sa" or service accounts**

[MartinT](https://www.sqlservercentral.com/author/martint), 2019-07-04 (first published: 2019-06-26)

FROM: <https://www.sqlservercentral.com/scripts/audit-users-logging-in-using-sa-or-service-accounts>

Security is probably one of a production DBA's most important tasks and if developers use application or service accounts to run queries in your production environment you need to identify then and prohibit it.

I notice some unwanted activity after staring a new job and decided to create a script that notifies me via email when this occurs. Triggers are not allowed in our production environment so I created a SQL Job that is scheduled to run every five minutes.

IF OBJECT\_ID ('AuditSqlLogins') IS NOT NULL DROP TABLE AuditSqlLogins

GO

CREATE TABLE AuditSqlLogins (

[Counter] [int] IDENTITY(1,1) NOT NULL,

[Login\_name] [varchar](20) NULL,

[host\_name] [varchar](20) NULL,

[login\_time] [datetime] NULL

) ON [PRIMARY]

INSERT INTO [dbo].[AuditSqlLogins]

(login\_time, login\_name, host\_name )

SELECT login\_time, login\_name, host\_name

FROM sys.dm\_exec\_sessions

WHERE host\_name not like '%APP%' -- excludeds Apllication server logins

and host\_name not like '%WWW%' -- excludeds Web server logins

and database\_id = 5 -- Specify the database you want to audit

and login\_name = 'Appadmin' -- specify the account you want audited

or login\_name = 'sa'

ORDER BY host\_name desc

DELETE FROM AuditSqlLogins

WHERE host\_name is null

DECLARE @counter integer

SELECT @counter = Counter FROM AuditSqlLogins

IF (@counter > 0)

BEGIN

DECLARE @xml NVARCHAR(MAX)

SET @xml = CAST ( ( SELECT

td = login\_name , '',

td = host\_name, '',

td = login\_time,''

FROM AuditSqlLogins

FOR XML PATH('tr'), TYPE

) AS NVARCHAR(MAX) )

DECLARE @body nvarchar(max);

SET @body ='

<html>

<body>

<head>

<style>

table {

border-collapse: collapse;

}

table, th, td {

border: 1px solid #ea5685;

}

</style>

</head>

<H3>Audit Apadmin and SA Login Event : (Server Name)</H3>

<table border="1" cellspacing="0" border-spacing="0" style ="text-align:center">

<tr style="height:15px; background:#ea8686">

<th border-spacing="0" style="padding:5px 15px;">login\_name</th>

<th border-spacing="0" style="padding:5px 15px;">host\_name</th>

<th border-spacing="0" style="padding:5px 15px;">login\_time</th>

</tr>

'

SET @body = @body+@xml+'</table><body>'

EXEC msdb.dbo.sp\_send\_dbmail

@recipients='youremail@yourwork.com',

@subject = 'Audit itsadmin and SA Login Event',

@body = @body,

@body\_format = 'HTML' ,

@profile\_name='Your DB Mail profile'

END

DROP TABLE AuditSqlLogins