عنوان: **محدود کردن دسترسی به اس کیوال سرور بر اساس IP**
نویسنده: وحید نصیری
تاریخ: ۱۳۸۸/۰۲/۱۰ ۲۱:۰۹:۰۰
آدرس: www.dotnettips.info
برچسب‌ها: SQL Server

عموما محدود کردن دسترسی بر اساس IP بهتر است بر اساس راه حل‌هایی مانند فایروال ، IPSec و یا RRAS IP Filter صورت گیرد که جزو بهینه‌ترین و امن‌ترین راه حل‌های ممکن هستند.
در ادامه قصد داریم این محدودیت را با استفاده از امکانات خود اس کیوال سرور انجام دهیم (بلاک کردن کاربران بر اساس IP های غیرمجاز). مواردی که در ادامه ذکر خواهند شد در مورد اس کیوال سرور 2005 ، سرویس پک 2 به بعد و یا اس کیوال سرور 2008 صادق است.
اس کیوال سرور این قابلیت را دارد که می‌توان بر روی کلیه لاگین‌های صورت گرفته در سطح سرور تریگر تعریف کرد . به این صورت می‌توان تمامی لاگین‌ها را برای مثال لاگ کرد (جهت بررسی مسایل امنیتی) و یا می‌توان هر لاگینی را که صلاح ندانستیم rollback نمائیم (ایجاد محدودیت روی لاگین در سطح سرور).

لاگ کردن کلیه لاگین‌های صورت گرفته به سرور

ایجاد جدولی برای ذخیره سازی اطلاعات لاگین‌ها:

```
USE [master]
GO

SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO

SET ANSI_PADDING ON
GO

CREATE TABLE [dbo].[Logging](
 [id] [int] IDENTITY(1,1) NOT NULL,
 [LogonTime] [datetime] NULL,
 [LoginName] [nvarchar](max) NULL,
 [ClientHost] [varchar](50) NULL,
 [LoginType] [varchar](100) NULL,
 [AppName] [nvarchar](500) NULL,
 [FullLog] [xml] NULL,
CONSTRAINT [PK_IP_Log] PRIMARY KEY CLUSTERED
(
 [id] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS  = ON,
ALLOW_PAGE_LOCKS  = ON) ON [PRIMARY]
) ON [PRIMARY]

GO

SET ANSI_PADDING OFF
GO

ALTER TABLE [dbo].[Logging] ADD  CONSTRAINT [DF_IP_Log_LogonTime]  DEFAULT (getdate()) FOR [LogonTime]
GO
```

در ادامه یک تریگر لاگین را جهت ذخیره سازی اطلاعات کلیه لاگین‌ها به سرور ایجاد می‌نمائیم:

```
USE [master]
GO

CREATE TRIGGER LogonTrigger
ON ALL SERVER
FOR LOGON
```

```
AS
BEGIN
   DECLARE @data XML
   SET @data = EVENTDATA()

   INSERT INTO [Logging]
     (
       [LoginName],
       [ClientHost],
       [LoginType],
       [AppName],
       [FullLog]
     )
   VALUES
     (
       @data.value('(/EVENT_INSTANCE/LoginName)[1]', 'nvarchar(max)'),
       @data.value('(/EVENT_INSTANCE/ClientHost)[1]', 'varchar(50)'),
       @data.value('(/EVENT_INSTANCE/LoginType)[1]', 'varchar(100)'),
       APP_NAME(),
       @data
     )
END
```

اکنون برای مثال از آخرین 100 لاگین انجام شده، به صورت زیر می‌توان گزارشگیری کرد:

```
SELECT TOP 100 *  FROM [master].[dbo].[Logging] ORDER BY id desc
```

و بدیهی است در تریگر فوق می‌توان روی هر کدام از آیتم‌های دریافتی مانند ClientHost و غیره فیلتر ایجاد کرد و تنها موارد مورد نظر را ثبت نمود.

محدود کردن کاربران بر اساس IP

ClientHost ایی که در رخداد لاگین فوق بازگشت داده می‌شود همان IP کاربر راه دور است. برای فیلتر کردن IP های غیرمجاز، ابتدا در دیتابیس مستر یک جدول برای ذخیره سازی IP های مجاز ایجاد می‌کنیم و IP های کلیه کلاینت‌های معتبر خود را در آن وارد می‌کنیم:

```
USE [master]
GO
CREATE TABLE [IP_RESTRICTION](
 [ValidIP] [varchar](15) NOT NULL,
CONSTRAINT [PK_IP_RESTRICTION] PRIMARY KEY CLUSTERED
(
 [ValidIP] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS  = ON,
ALLOW_PAGE_LOCKS  = ON) ON [PRIMARY]
) ON [PRIMARY]
```

سپس تریگر لاگین ما برای منع کاربران غیرمجاز بر اساس IP ، به صورت زیر خواهد بود:

```
USE [master]
GO

CREATE TRIGGER [LOGIN_IP_RESTRICTION]

ON ALL SERVER
FOR LOGON
AS
BEGIN
   DECLARE @host NVARCHAR(255);
   SET @host = EVENTDATA().value('(/EVENT_INSTANCE/ClientHost)[1]', 'nvarchar(max)');

   IF (
          NOT EXISTS(
              SELECT *
              FROM   MASTER.dbo.IP_RESTRICTION
```

```
            WHERE  ValidIP = @host
        )
    )
BEGIN
        ROLLBACK;
END
END;
```

اخطار مهم!
تریگر فوق خطرناک است! ممکن است خودتان هم دیگر نتوانید لاگین کنید!! (حتی با اکانت ادمین)
بنابراین قبل از لاگین حتما IP لوکال و یا ClientHost لوکال را هم وارد کنید.
اگر گیر افتادید به صورت زیر می‌شود رفع مشکل کرد:
تنها حالتی که تریگر لاگین را فعال نمی‌کند Dedicated Administrator Connection است یا DAC هم به آن گفته می‌شود. به صورت پیش فرض برای ایجاد این اتصال اختصاصی باید به کامپیوتری که اس کیوال سرور بر روی آن نصب است به صورت لوکال لاگین کرد و سپس در خط فرمان دستور زیر را صادر کنید (حرف A آن باید بزرگ باشد):

```
C:\>sqlcmd -A -d master -q "insert into IP_RESTRICTION(validip) values('<local machine>')"
```

به این صورت local machine به جدول IP های مجاز اضافه شده و می‌توانید لاگین کنید!
این نوع تریگرها در قسمت server objects در management studio ظاهر می‌شوند.

نظرات خوانندگان

نویسنده: مجید
تاریخ: ۱۳۹۱/۰۶/۲۹ ۱۱:۵۶

سلام جناب نصیری
مقاله بسیار جالبی بود.(حتی با اینکه متعلق به سه سال پیش بود)
بر اساس مقاله، تریگری برای لاگ کردن تمامی لاگین‌ها به سرور ایجاد کردم. اما به یک مشکل برخوردم:اگر لاگین sysAdmin باشد مشکلی نخواهیم داشت اما اگر تنها public باشد در هنگام لاگین با خطا مواجه خواهیم شد:

```
Logon failed for login 'm' due to trigger execution.
```

```
Changed database context to 'master'.
```

```
Changed language setting to us_english. (Microsoft SQL Server, Error: 17892)
```

آیا راه حلی وجود دارد؟متاسفانه من نتوانستم راه حلی پیدا کنم.
با تشکر...

نویسنده: وحید نصیری
تاریخ: ۱۳۹۱/۰۶/۲۹ ۱۲:۲۶

باید دسترسی به سرور شما داشت تا بشود اظهار نظر کرد. دسترسی‌ها چی هست. یوزرها به چه بانک‌های اطلاعاتی دسترسی دارند و مسایلی از این دست که از راه دور قابل بررسی نیست.
ولی درکل در اینجا از دیتابیس سیستمی master برای ساخت جدول Logging استفاده شده. این رو تغییر بدید به یک دیتابیس دیگر با سطح دسترسی عمومی.

```
USE [dbName]
go
INSERT INTO [dbName].schemaName.[Logging]
...
```