دوره آموزش امنیت در SQL Server 2022

طول دوره: ۲۰ ساعت

مدرس: مسعود طاهری

مدرس: مسعود طاهری

عنـــوان دوره: **دوره آموزش امنیت در SQL Server ۲۰۲۲**

موضوع: امنیت در SQL Server ۲۰۲۲

مخـــاطبین: علاقه‌مندان به مباحث امنیت در SQL Server

طـــول دوره: **۱۵ الی ۲۰ ساعت**

نحـــوه ارائه: **به‌صورت غیرحضوری**

مـــــدرس: مسعود طاهری

پشتیبانی: گروه تلگرامی پشتیبانی

نوع ارائه: انتشار جلسات به صورت هفتگی

دارای گواهی دیجیتال شرکت در دوره

دسترسی از طریق پلیر اختصاصی اسپات پلیر

روش مشاهده دوره‌های آموزشی محافظت شده

مدرس این دوره کیست؟

مسعود طاهری، مدرس و مشاور ارشد SQL Server & BI

مسعود طاهری مدرس و مشاور ارشد SQL Server & BI ، مدیر فنی پروژه‌های هوش تجاری (بیمه سامان، اوقاف، جین وست، هلدینگ ماهان و...) ، مدرس دوره‌هـــای SQL Server و هوش‌تجاری در شرکت نیک‌آموز و نویسنده کتاب PolyBase در SQL Server

دوره آموزشی امنیت در SQL Server از نیمه دوم اردیبهشت ماه شروع می‌شود و جلسات به صورت هفتگی در استودیو اختصاصی نیک‌آموز ضبط و منتشر می‌گردد.

مدرس: مسعود طاهری

مدل‌های ثبت‌نام این دوره:

بنا به نیاز و درخواست دانشجویان، دو نوع ثبت‌نام برای این دوره در نظر گرفته‌ایم که هر کدام شامل موارد به خصوصی می‌شوند.

	پنل نقره‌ای	پنل طلایی
آموزش ویدئویی دوره امنیت در SQL Server	✅	✅
ارائه ابزار تخصصی برای Block کردن حملات Brute-Force درSQL Server	✅	✅
آموزش ویدئویی فارسی ابزار تخصصی Block کردن حملات Brute-Force	✅	✅
ارائه اسکریپت های پرکاربرد در حوزه امنیت SQL Servere	✅	✅
آموزش و ارائه برنامه PsExec و نحوه استفاده از آن در سناریوهای SQL Server	✅	✅
آموزش و ارائه ابزار جهت مانتیور کردن ترافیک SQL Server در شبکه	✅	✅
آموزش و ارائه ابزار برای Recovery رمز عبور Loginها در SQL Server	✅	✅
آموزش و ارائه ابزار در جهت مشاهده کدهای CLR Object در SQL Server	✅	✅
آموزش و ارائه ابزار در جهت فرمان به سرور های دیگر با استفاده از SQL Server	✅	✅
گروه تلگرامی پرسش و پاسخ	✅	✅
دو جلسه ۶۰ دقیقه‌ای پرسش و پاسخ در حوزه امنیت در SQL Server	✅	✅
آموزش فارسی Idera SQL Secure	❌	✅
آموزش فارسی Idera SQL Compliance Manager	❌	✅
یک جلسه مشاوره ۶۰ دقیقه‌ای با تیم فنی نیک آموز	❌	✅
نصب و استقرار دو نرم‌افزار با تیم فنی نیک آموز	❌	✅
ارائه گزارش عارضه یابی امنیت دیتابیس با تیم نیک آموز	❌	✅

کسب اطلاعات برای پیش ثبت نام و ارتباط با تیم مشاوران نیک آموز:

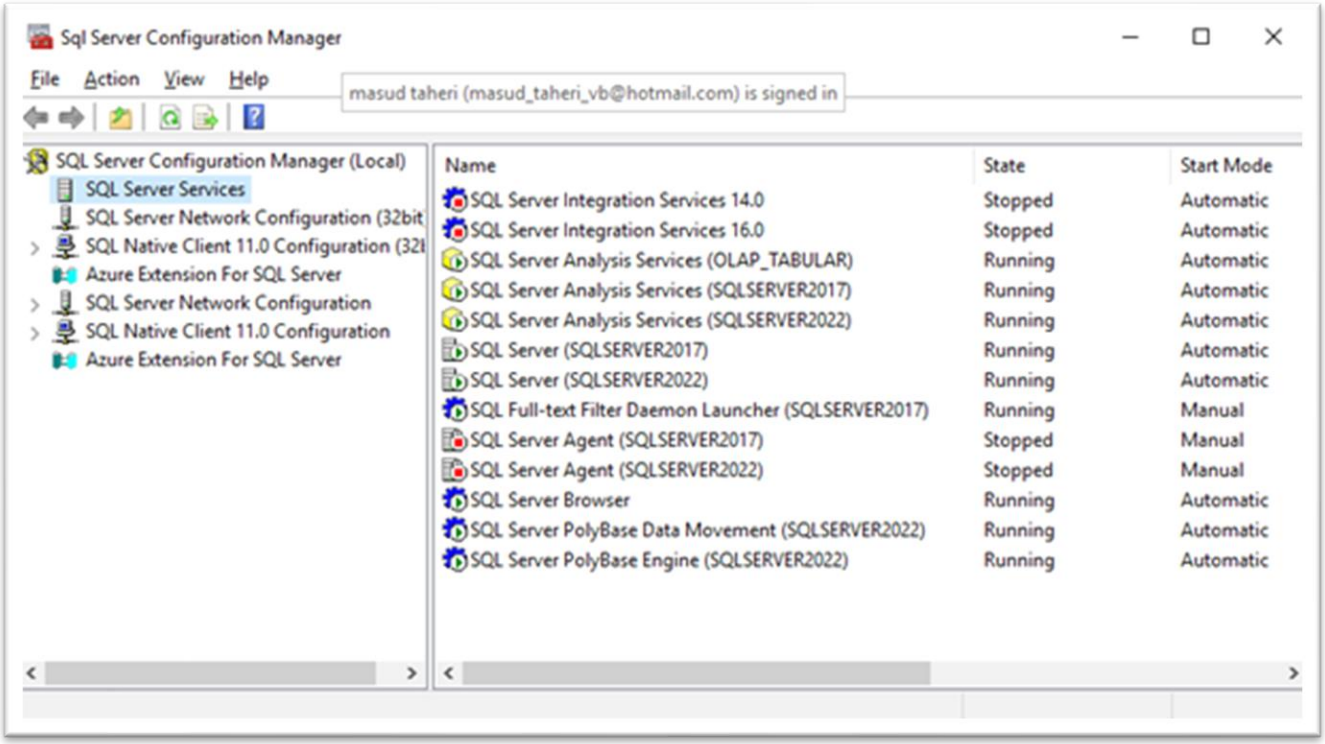
دریافت مشاوره رایگان

مدرس: مسعود طاهری

بخش اول: تعاریف و مفاهیم اولیه

- بررسی اهداف پیاده‌سازی امنیت
- معرفی مفهوم Authentication
- معرفی مفهوم Authorization
- معرفی اولیه Windows Authentication
- معرفی اولیه SQL Server Authentication
- معرفی اولیه مفهوم Login
- معرفی اولیه مفهوم User
- معرفی اولیه مفهوم Windows Service
- معرفی اولیه برنامه Services ویندوز و نحوه کارکردن با آن
- معرفی برنامه SQL Serer Configuration Manager
- معرفی برنامه Windows Event Viewer
- معرفی برنامه MMC و نحوه کار با آن
- معرفی برنامه Windows Service Manger و نحوه کار با آن
- بررسی نحوه تعریف و مدیریت کاربران در سیستم عامل ویندوز
- بررسی نحوه اجرای برنامه‌ها در ویندوز با دسترسی کاربران مختلف
- آشنایی با برنامه Group Policy در سیستم عامل ویندوز
- معرفی اولیه Power Shell و نحوه کار با آن
- معرفی اولیه Command Prompt و نحوه کار با آن
- بررسی نحوه Impersonate کردن Command Prompt
- معرفی مفهوم Instance در SQL Server
- بررسی مفهوم Default Instance در SQL Server
- بررسی مفهوم Named Instance در SQL Server
- آشنایی با مفهوم Stored Procedure های سیستمی
- آشنایی با مفهوم Dynamic Management View های سیستمی
- آشنایی با مفهوم Function های سیستمی

برنامه SQL Server Configuration Manager که به‌همراه SQL Server نصب می‌گردد، یکی از برنامه‌های قدرتمند مدیریت سرویس‌های SQL Server است. برخی از نکات مربوط به حوزه امنیت و همچنین حوزه Performance در SQL Server توسط این برنامه باید تنظیم گردد. همیشه در طی پروژه‌ها و آموزش‌هایی که انجام می‌دهیم، به کار کردن اصولی با این برنامه تأکید ویژه‌ای داشتم.

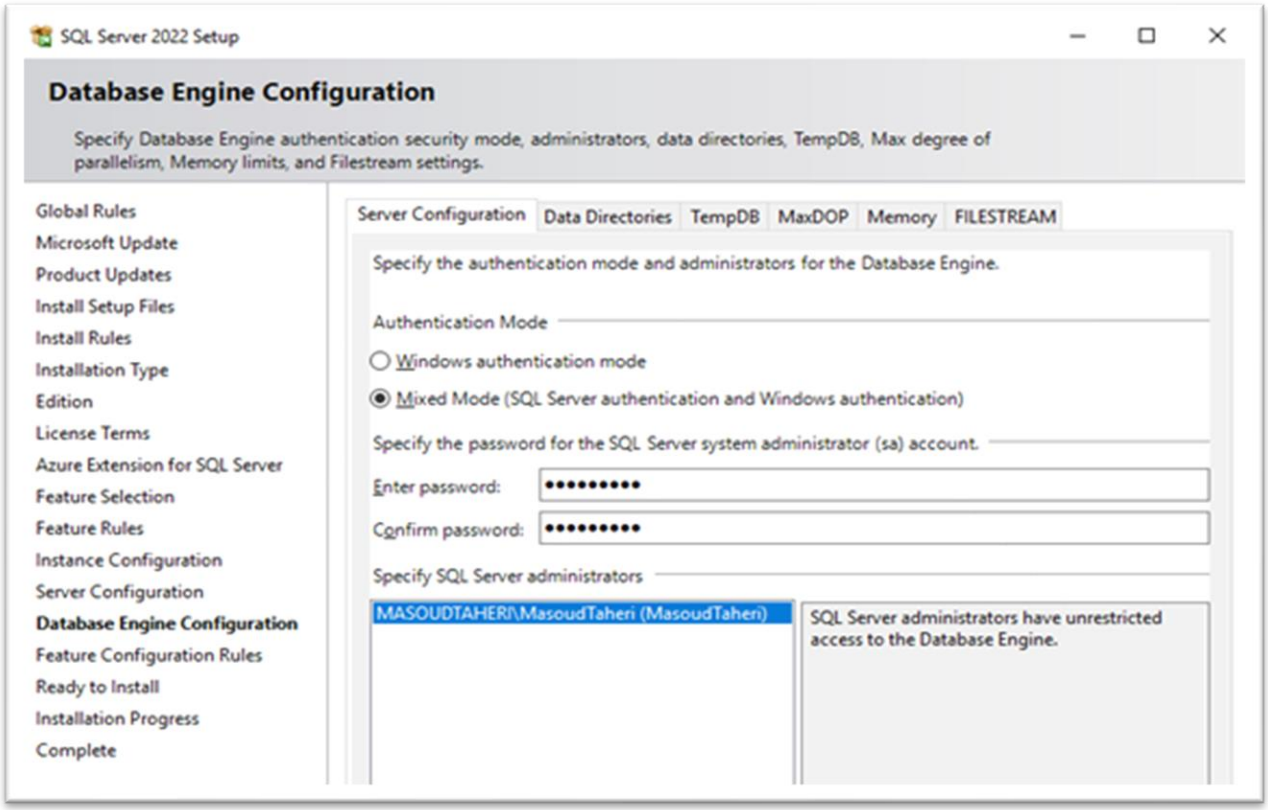


مدرس: مسعود طاهری

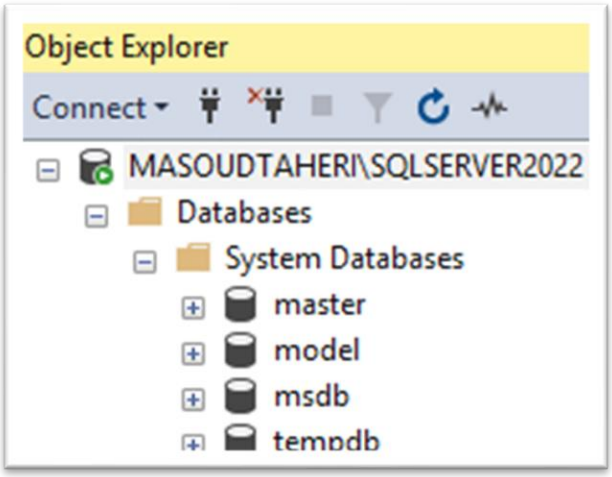
بخش دوم: نصب یک نسخه از SQL Server به‌صورت اَمن

- معرفی نسخه‌های SQL Server
- بررسی نحوه نصب SQL Server امن برروی یک سرور
- بررسی نحوه نصب سرویس SSIS
- بررسی نحوه نصب سرویس SSAS
- بررسی بخش‌های مختلف SQL Server هنگام نصب
- بررسی تنظیمات Account های راه‌انداز سرویس هنگام نصب
- نکات مهم درخصوص تغییر نام سرور مربوط به SQL Server
- بررسی Authentication Mode و تنظیمات مربوط به آن هنگام نصب

برای نصب امن یک نسخه از SQL Server باید یکسری نکات را رعایت کرد. ما در طی این دوره، نکات کاربردی و مهمی درخصوص نصب SQL Server به‌صورت امن را به شما آموزش خواهیم دا



بخش سوم: بررسی بانک‌های اطلاعاتی سیستمی



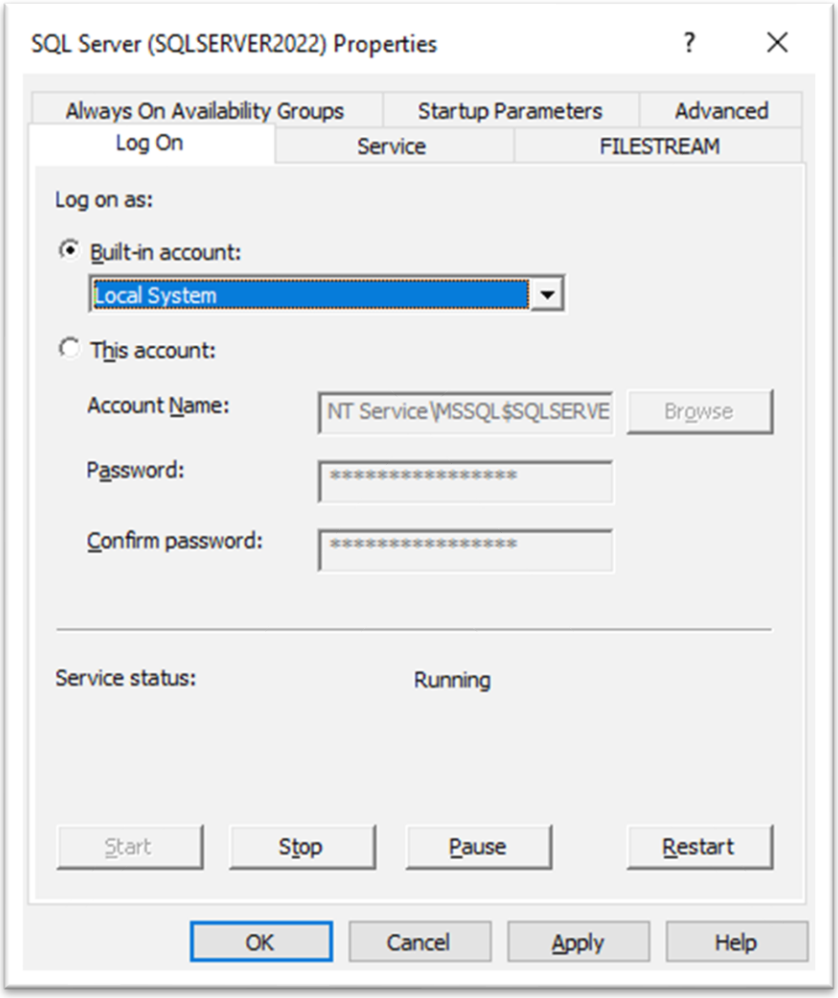
- بررسی کاربرد بانک‌های اطلاعاتی سیستمی
- بررسی بانک اطلاعاتی سیستمی master
- بررسی بانک اطلاعاتی سیستمی msdb
- بررسی بانک اطلاعاتی سیستمی tempdb
- بررسی بانک اطلاعاتی سیستمی model
- بررسی بانک اطلاعاتی سیستمی resourcedb

یکی از بانک‌های اطلاعاتی مهم و کاربردی که مهم‌ترین تنظیمات امنیتی SQL Server برروی آن ذخیره می‌گردد، بانک اطلاعاتی master است. در طی این دوره، با جداول مهم این بانک اطلاعاتی آشنا شده و نقش آن در امنیت SQL Server را بررسی خواهیم کرد.

بخش چهارم: بررسی اولیه سرویس‌های SQL Server و امن‌سازی آن‌ها

- بررسی سرویس اصلی SQL Server
- بررسی سرویس Agent
- بررسی سرویس SSIS
- بررسی سرویس SSAS
- بررسی سرویس Full Text Search
- بررسی سرویس PolyBase
- بررسی سرویس SQL Server Browser
- بررسی سرویس CEIP در SQL Server و نکات امنیتی مربوط به آن
- بررسی فعال و غیرفعال‌سازی سرویس‌های وابسته به SQL Server
- بررسی تأثیر فعال و یا غیرفعال‌بودن سرویس‌های SQL Server در امنیت آن
- بررسی نحوه تنظیم Account های راه‌انداز برای سرویس‌های SQL Server
- بررسی نحوه راه‌اندازی سرویس‌های SQL Server با استفاده از Local System
- بررسی نحوه راه‌اندازی سرویس‌های SQL Server با استفاده از Local Service
- بررسی نحوه راه‌اندازی سرویس‌های SQL Server با استفاده از Network Service
- بررسی نحوه راه‌اندازی سرویس‌های SQL Server با استفاده از Virtual Account
- معرفی MSA Account ها و نحوه راه‌اندازی سرویس‌های SQL Server با استفاده از آن
- معرفی GMSA و نحوه راه‌اندازی سرویس‌های SQL Server با استفاده از آن
- بررسی تعریف Custom Account و نحوه راه‌اندازی سرویس‌های SQL Server با استفاده از آن
- بررسی Permission های لازم برای راه‌اندازی Custom Account
- نحوه اعمال دسترسی برای ذخیره نسخه پشتیبان SQL Server تحت شبکه به‌صورت Domain
- نحوه اعمال دسترسی برای ذخیره نسخه پشتیبان SQL Server تحت شبکه به‌صورت Workgroup
- معرفی اولیه دستور Net و نحوه مدیریت سرویس‌های SQL Server با استفاده از آن

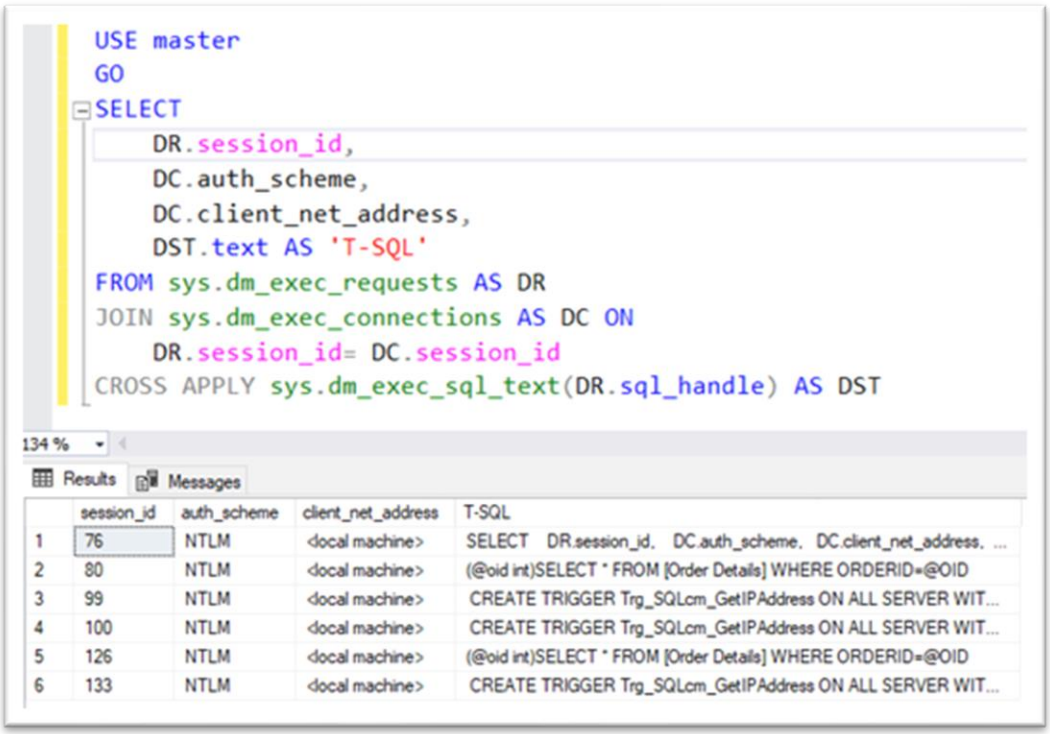
برای راه‌اندازی سرویس‌های SQL Server نیاز به اکانت راه‌انداز (Log on) است. تنظیمات مربوط به این بخش، به‌شدت مهم است. متأسفانه در حال حاضر، برخی از ادمین‌ها، سرویس SQL Server را با Local System استارت می‌زنند و اصلاً به فکر امنیت سرورهای خود نیستند. ما در نیک آموز موارد مربوط به این حوزه را به‌خوبی بررسی خواهیم کرد.



بخش پنجم: بررسی Session ها در SQL Server

- بررسی مفهوم Session در SQL Server
- آشنایی با Procedure های سیستمی جهت کار با Session ها
- آشنایی با Function های سیستمی جهت کار با Session ها
- آشنایی با DMV های سیستمی جهت کار با Session ها
- بررسی Context Info و تنظیمات آن در SQL Server
- بررسی نحوه مشاهده هرکدام از دستورات اجراشده توسط Session ها
- بررسی نحوه مانیتور کردن Session ها در SQL Server
- بررسی روش‌های ارسال مشخصات Business User به SQL Server
- بررسی Kill کردن Session ها و نکات مربوط به آن

ما در SQL Server می‌توانیم لیست Session هایی که به آن متصل شده و درحال اجرای دستورات هستند را به‌دست آوریم و دستورات آن‌ها را مشاهده کنیم. این موضوع باعث می‌شود که ما بتوانیم راحت‌تر سرور خود را از لحاظ امنیتی مانیتور کنیم. برای این منظور، می‌توان از DMV های کاربردی سیستمی استفاده کرد.



```
USE master
GO
SELECT
    DR.session_id,
    DC.auth_scheme,
    DC.client_net_address,
    DST.text AS 'T-SQL'
FROM sys.dm_exec_requests AS DR
JOIN sys.dm_exec_connections AS DC ON
    DR.session_id= DC.session_id
CROSS APPLY sys.dm_exec_sql_text(DR.sql_handle) AS DST
```

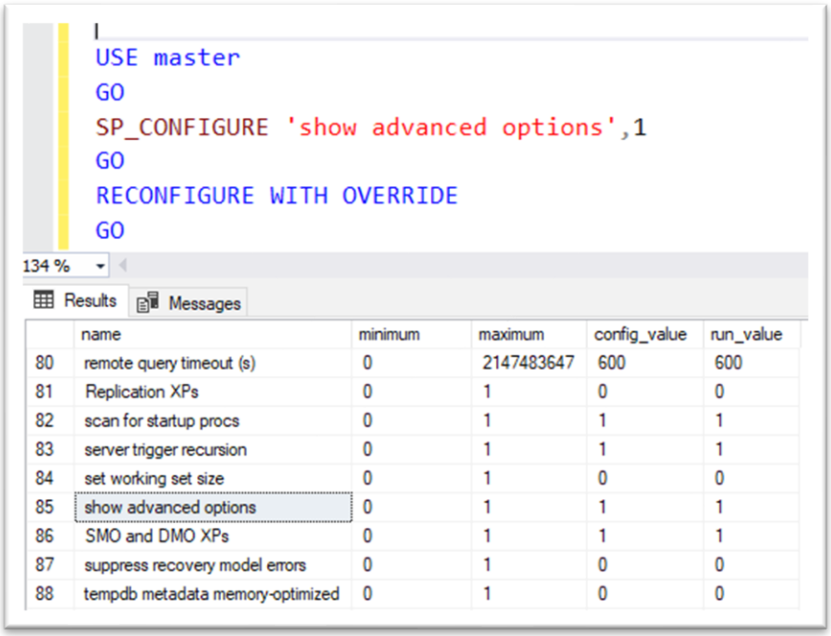
134 %

Results | Messages

	session_id	auth_scheme	client_net_address	T-SQL
1	76	NTLM	<local machine>	SELECT DR.session_id, DC.auth_scheme, DC.client_net_address, ...
2	80	NTLM	<local machine>	(@oid int)SELECT * FROM [Order Details] WHERE ORDERID=@OID
3	99	NTLM	<local machine>	CREATE TRIGGER Trg_SQLcm_GetIPAddress ON ALL SERVER WIT...
4	100	NTLM	<local machine>	CREATE TRIGGER Trg_SQLcm_GetIPAddress ON ALL SERVER WIT...
5	126	NTLM	<local machine>	(@oid int)SELECT * FROM [Order Details] WHERE ORDERID=@OID
6	133	NTLM	<local machine>	CREATE TRIGGER Trg_SQLcm_GetIPAddress ON ALL SERVER WIT...

بخش ششم: بررسی بخش تنظیمات پیشرفته SQL Server (کار با پروسیجر SP_Configure)

- بررسی بخش تنظیمات پیشرفته SQL Server
- بررسی نحوه استفاده از پروسیجر سیستمی SP_Configure
- بررسی نحوه فعال و غیرفعال‌سازی تنظیمات پیشرفته
- بررسی تنظیمات مفید امنیتی در بخش تنظیمات پیشرفته



```
USE master
GO
SP_CONFIGURE 'show advanced options',1
GO
RECONFIGURE WITH OVERRIDE
GO
```

134 %

Results | Messages

	name	minimum	maximum	config_value	run_value
80	remote query timeout (s)	0	2147483647	600	600
81	Replication XPs	0	1	0	0
82	scan for startup procs	0	1	1	1
83	server trigger recursion	0	1	1	1
84	set working set size	0	1	0	0
85	show advanced options	0	1	1	1
86	SMO and DMO XPs	0	1	1	1
87	suppress recovery model errors	0	1	0	0
88	tempdb metadata memory-optimized	0	1	0	0

یکی از بخش‌های جذاب SQL Server ، کار کردن با قسمت تنظیمات مربوط به آن است. برای کار با تنظیمات پیشرفته در SQL Server می‌توان از پروسیجر سیستمی sp_configure استفاده کرد. ما در طی این دوره، نحوه کار با این پروسیجر و تنظیم‌های مهم امنیتی SQL Server را به شما آموزش خواهیم داد.

بخش هفتم: بررسی Connection String و تنظیمات امنیتی مربوط به آن

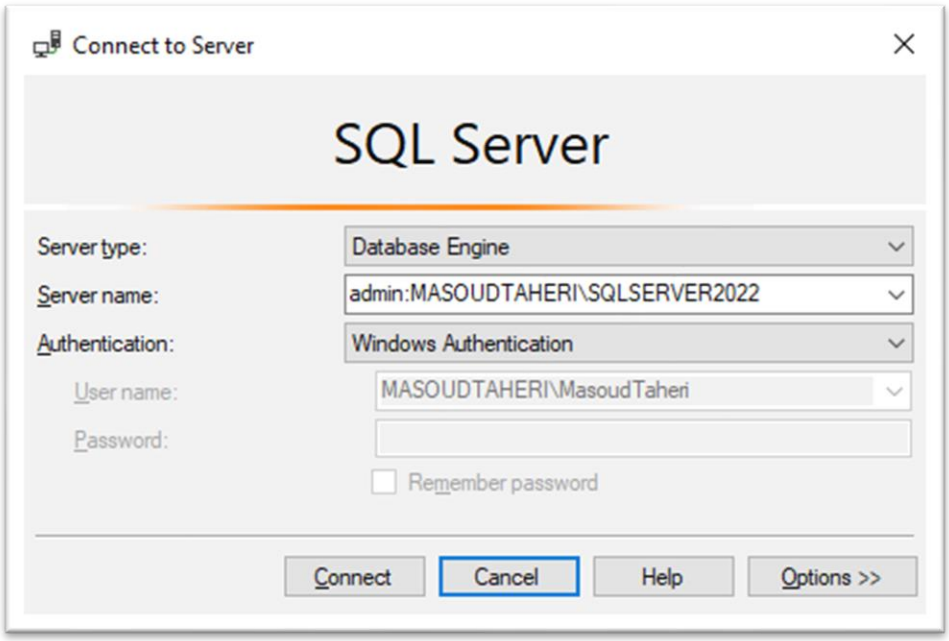
- بررسی مفهوم Connection String
- بررسی اجزاء مهم Connection String
- بررسی تکنیک‌های امن‌کردن Connection String
- بررسی ارسال داده اضافی به‌همراه Connection String به SQL Server
- بررسی امن‌کردن Connection String در دات نت

چند سال پیش یکی از شرکت‌هایی که با آن‌ها پروژه داشتیم، دنبال روشی برای ارسال Business User به‌همراه Connection String به بانک اطلاعاتی بود. روشی که خود آن‌ها استفاده کرده بودند، استفاده از پارامتر Application Name بود. اما این موضوع باعث به‌وجود آمدن مشکلاتی مانند Connection Pooling و... شده بود. برای رفع مشکلات مربوط به این موضوع، ما استفاده از Context Info را به آن‌ها پیشنهاد دادیم. استفاده از Context Info در سناریوهایی که امنیت برای آن‌ها مهم بوده، کاربردی است.

بخش هشتم: بررسی تنظیمات پیشرفته SQL Server جهت اتصال

- بررسی DAC Connection
- بررسی نحوه استفاده از DAC Connection در SQL Server
- بررسی نحوه Single Mode کردن سرویس SQL Server
- بررسی سوئیچ‌های کاربردی سرویس اصلی SQL Server
- بررسی نحوه اتصال به SQL Server بدون داشتن Login Name و Password

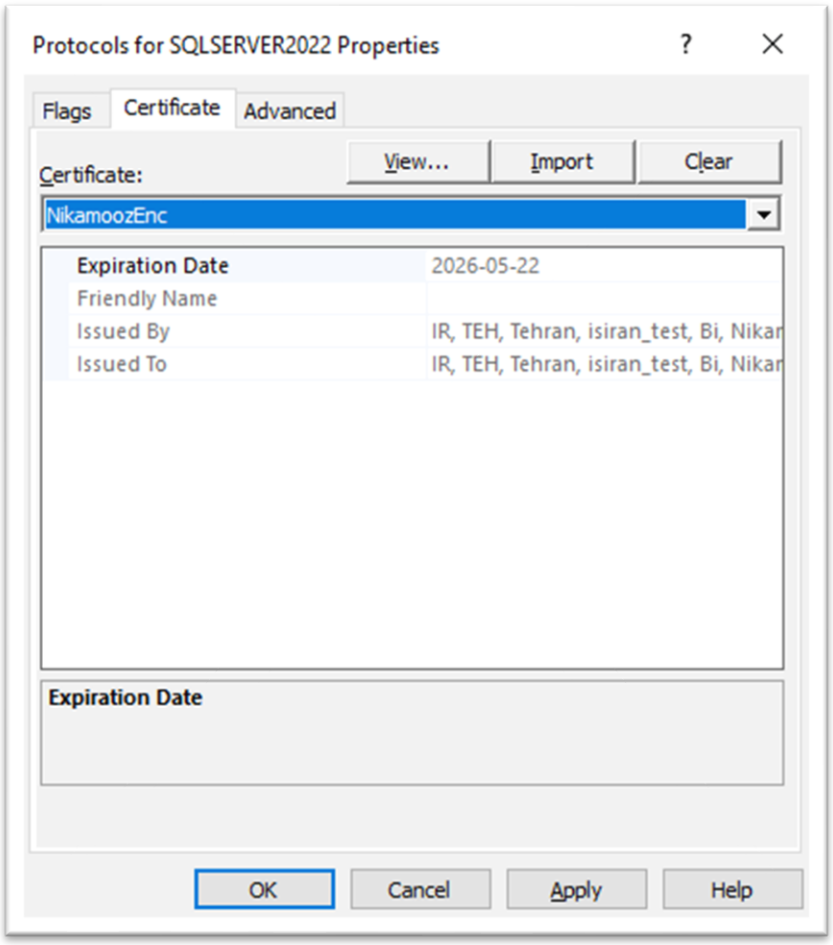
در برخی سرور SQL Server به‌طور وحشتناکی Busy است که امکان پاسخ‌دهی به کاربران و همچنین اتصال به آن، به‌سختی فراهم است. در این حالت، حتی به‌راحتی نمی‌توان به سرور Remote زد و یا با استفاده از SSMS ازطریق یک کلاینت به SQL Server متصل شد. خیلی از کاربران در چنین مواقعی، ماشین مجازی مربوط به سرور را Reset می‌کنند. اما یک راهکار دیگر برای اتصال به SQL Server و انجام کارهای مدیریتی وجود دارد و آن استفاده از Dedicate Administrator Connection است که به اختصار به آن DAC می‌گویند. من از این ویژگی در سرورهایی که احتمال می‌دهم به علت حجم درخواست‌ها ممکن است Busy شوند، استفاده می‌کنم.



بخش نهم: بررسی نحوه امن‌کردن لایه انتقال داده

- آشنایی با مفهوم TCP Port و اعمال تنظیمات مربوط به آن
- بررسی TCP Port های لازم برای کار با SQL Server
- بررسی نحوه پیداکردن Instance های نصب‌شده در SQL Server
- بررسی Firewall و نحوه تنظیم آن برای SQL Server
- بررسی TLS و انجام تنظیمات مربوط به آن در SQL Server
- بررسی تنظیمات مربوط به Extended Protection در SQL Server

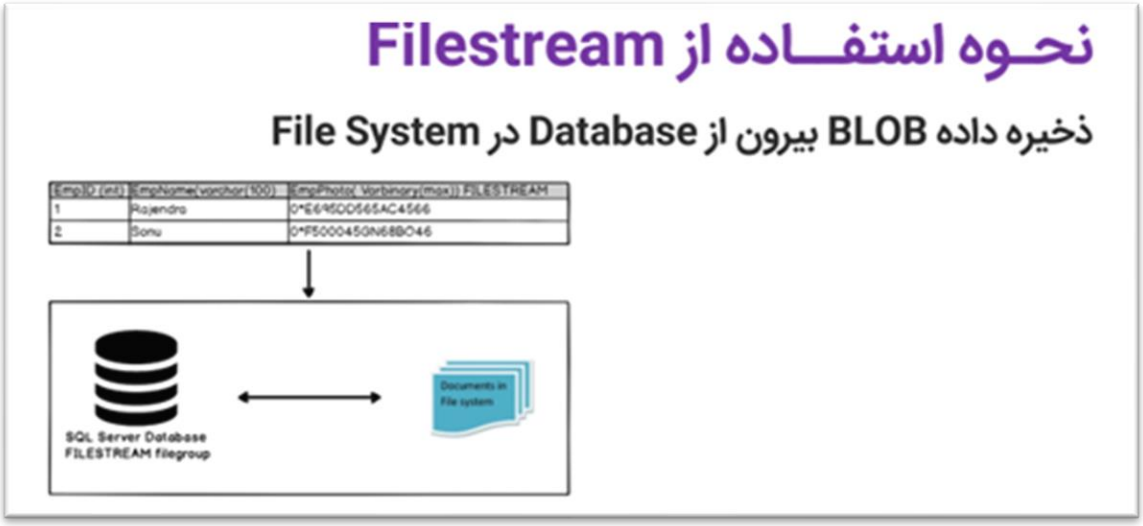
مدرس: مسعود طاهری



به‌طور خیلی ساده، TLS یک پروتکل برای رمزکردن داده‌ها در بستر ارتباطی است. به وسیله این پروتکل، زمانی که کلاینت به SQL Server متصل می‌شود، داده‌هایی که در بستر شبکه ارسال می‌شوند با استفاده از این پروتکل رمز می‌شوند. چند وقت پیش تیم ما یک تجربه جالب برای استفاده از این موضوع برروی سرور یک Application ویندوزی قدیمی داشت که برای امن‌سازی داده‌هایی که در سطح شبکه (اینترنت داخلی) درحال استفاده بود، از آن استفاده کردیم.

بخش دهم: بررسی Filestream

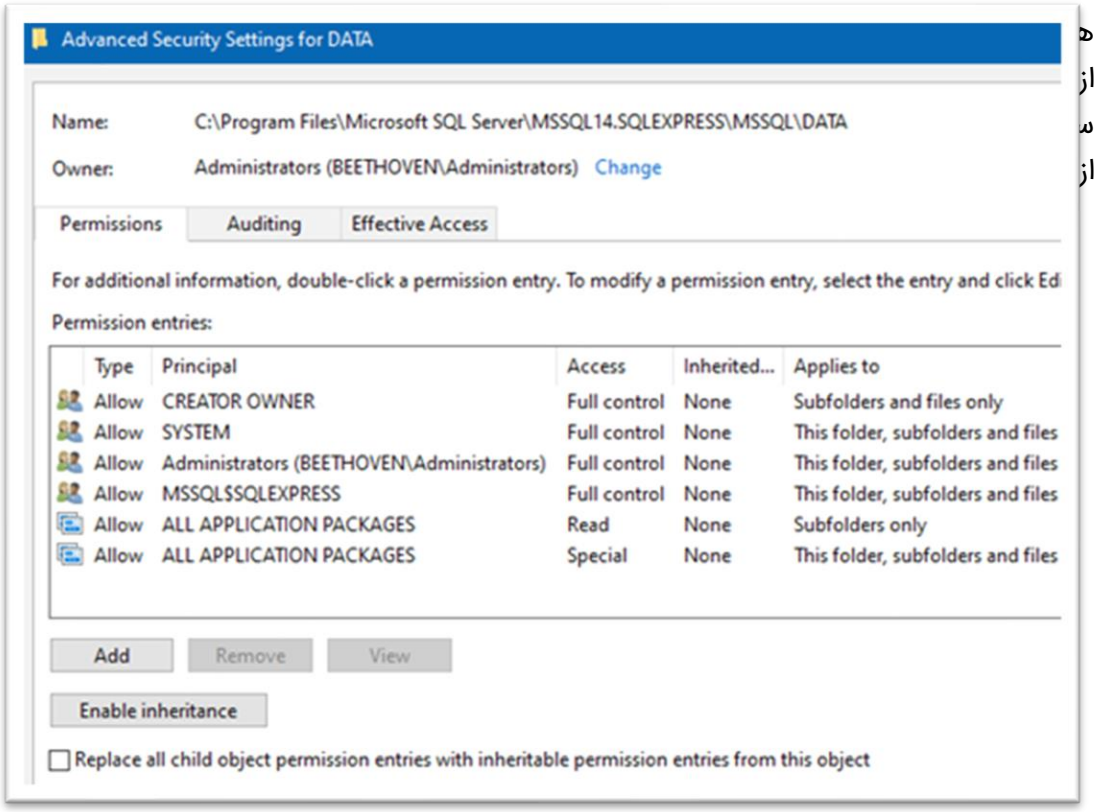
- بررسی نحوه فعال‌سازی Filestream
- ایجاد بانک‌های اطلاعاتی Filestream
- بررسی امنیت SQL Server هنگام کار با Filestream
- بررسی Filetable و نکات امنیتی مربوط به آن
- بررسی Encrypt کردن فایل‌های ذخیره‌شده با تکنولوژی‌های Filestream



تکنولوژی Filestream در SQL Server جهت مدیریت ذخیره و بازیابی BLOB است. اگر شما می‌خواهید تصویر، فایل Word، فایل PDF و... را در SQL Server ذخیره کنید، ویژگی Filestream و تکنولوژی‌های وابسته به آن می‌تواند برای شما مناسب باشد. زمانی که از Filestream استفاده می‌کنید، باید حواستان به امنیت فایل‌های ذخیره‌شده به‌وسیله این تکنولوژی باشد. ما در طی این دوره، نکات کاربردی درخصوص امنیت این تکنولوژی به شما ارائه خواهیم کرد.

بخش یازدهم: امن‌سازی فایل‌های بانک اطلاعاتی در سطح سیستم عامل

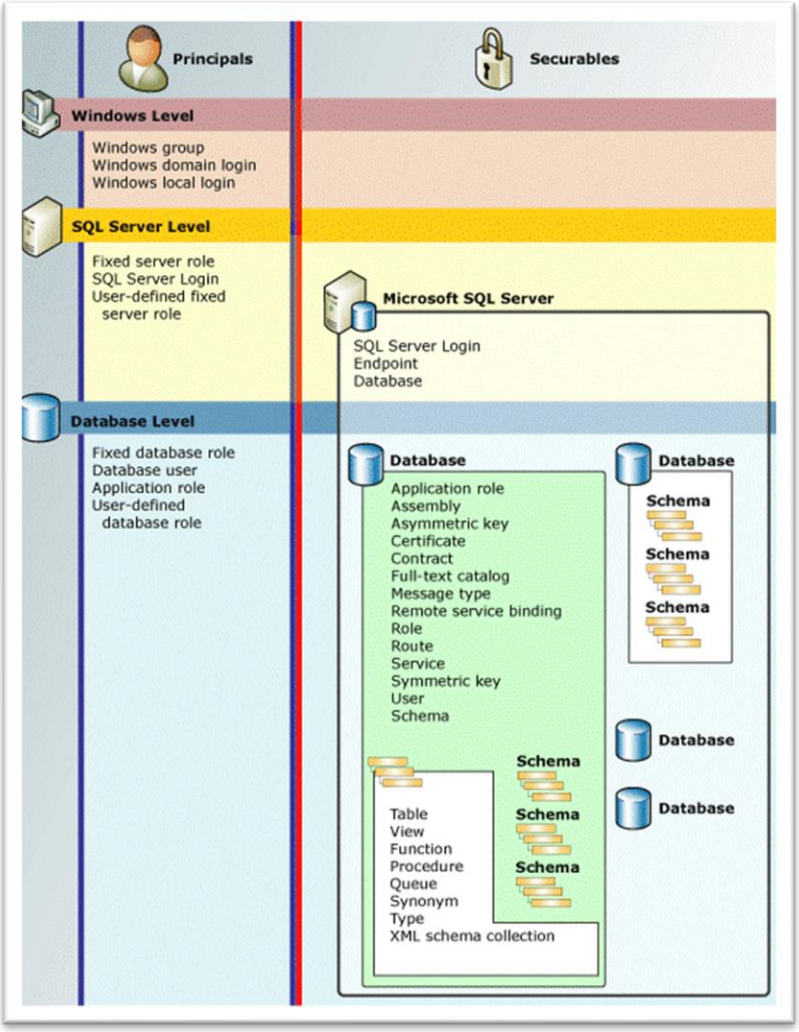
- بررسی امنیت Data File ها
- بررسی امنیت Log File ها
- بررسی Permission ه
- بررسی تأثیر استفاده از
- بررسی Bitlocker در س
- بررسی تأثیر استفاده از



هر بانک اطلاعاتی، از حداقل دو فایل تشکیل شده است. یکی از این فایل‌ها Data File و دیگری Log File است که ما در سطح سیستم عامل، با انجام تنظیمات مناسبی می‌توانیم امنیت فایل‌های مربوط به SQL Server را به‌صورت مناسب تأمین نماییم. در طی این دوره، شما با تکنیک‌های کاربردی در این خصوص آشنا خواهید شد.

بخش دوازدهم: بررسی مفاهیم اولیه Security در SQL Server

- بررسی مفهوم Principal
- بررسی سطوح Principle در سطح ویندوز و SQL Server و Database
- بررسی مفهوم Securable
- بررسی مفهوم Permission
- بررسی ساختار امنیتی SQL Server
- بررسی مفهوم Instance Level Security
- بررسی مفهوم Database Level Security
- بررسی سلسله‌مراتب امنیت و دسترسی در SQL Server
- بررسی تفاوت‌های Login و User



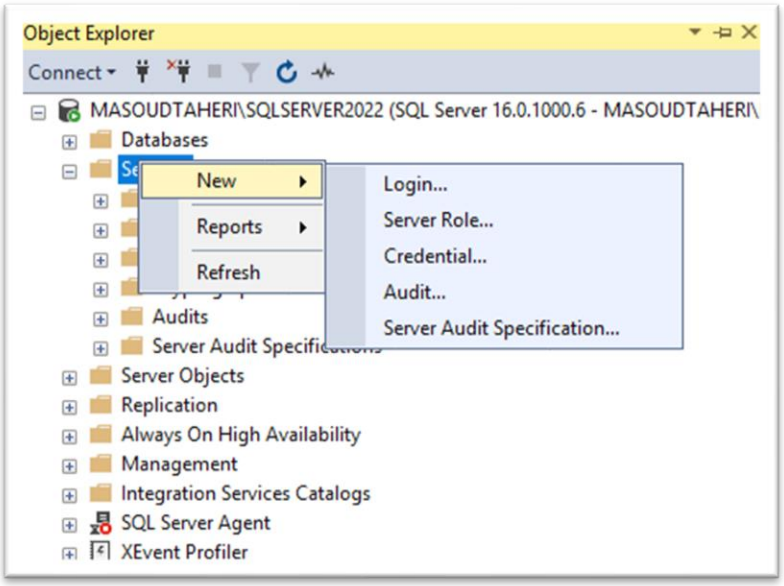
چند نکته و اصل کاربردی در حوزه امنیت SQL Server وجود دارد که شما باید به‌عنوان کسی که در این حوزه کار می‌کند، آن‌ها را بدانید. یادگیری این مفهوم با استفاده از سلسله‌مراتب امنیت و دسترسی در SQL Server امکان‌پذیر است. ما در طی این دوره، مباحث مربوط به این حوزه را به‌خوبی به شما یاد خواهیم داد.

مدرس: مسعود طاهری

بخش سیزدهم: بررسی Login

- بررسی نحوه تعریف Login
- بررسی انواع Login ها در SQL Server
- بررسی نحوه تنظیم Password Policy برای SQL Server
- بررسی نحوه اعطای مجوز به Login ها
- بررسی نحوه گرفتن مجوز از Login ها
- بررسی دستورات Grant، Revoke، Deny
- بررسی نحوه تخصیص دسترسی‌های مختلف به Login ها
- بررسی سناریوهای کاربردی درخصوص تخصیص دسترسی به Login ها
- بررسی نحوه Impersonate کردن به دسترسی یک Login
- بررسی Map شدن بین لاگین‌ها و User ها پس از Restore بانک اطلاعاتی
- بررسی نحوه انتقال لاگین‌های یک سرور به یک سرور دیگر
- بررسی مفهوم SID و نکات مربوط به آن
- بررسی مفهوم Brute-Force Attack و ارائه راه حل برای آن در SQL Server
- بررسی دلایل غیرفعال‌کردن لاگین SA در SQL Server
- بررسی مباحث مربوط به Cross Database Security
- بررسی توابع، DMF، DMV و SP های مربوط به این حوزه
- بررسی اعمال تنظیمات مناسب برای Owner بانک‌های اطلاعاتی و سایر اشیاء
- بررسی Server Permission های جدید در نسخه جدید SQL Server

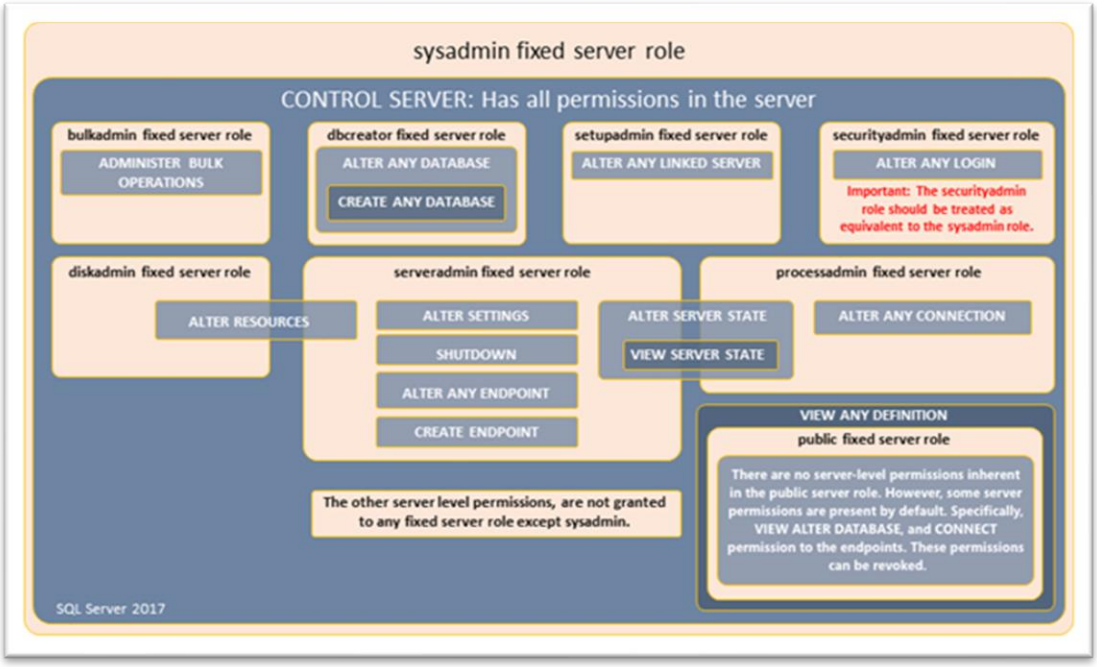
اولین گام جهت اتصال به SQL Server ، داشتن یک لاگین معتبر است. زمانی که شما Login تعریف می‌کنید، درگیر مباحث مانند Password Policy، Server Role و... هستید. یکی از اشتباهاتی که اکثر کاربران در این حوزه انجام می‌دهند، این است که یک Login تعریف و نقش آن را به‌عنوان Sys Admin درنظر گرفته و در اختیار سایر کاربران قرار می‌دهند. توصیه ما به شما این است که به هیچ عنوان به هر لاگینی نقش Sys Admin در Server SQL ارائه ندهید؛ مخصوصاً لاگین مربوط به Application ها. اگر شما برای یک Application لاگینی با نقش Sys Admin ایجاد کنید، نفوذ به SQL Server خود را راحت‌تر کرده‌اید.



بخش چهاردهم: بررسی Server Role

- معرفی مفهوم Role و انواع آن
- بررسی Server Role
- بررسی انواع Server Role ها در SQL Server
- بررسی نحوه ایجاد Server Role ها سفارشی در SQL Server
- بررسی DMV های مربوط به Server Role ها
- بررسی Server Role های جدید در نسخه جدید SQL Server
- بررسی DMV های مربوط به Server Role ها

در SQL Server نقش‌های ازپیش تعریف‌شده برای Login ها وجود دارد که دارای دسترسی‌هایی در حوزه‌های مختلف هستند. استفاده از این نقش‌ها می‌تواند باعث مدیریت اصولی و بهبود فرآیند دسترسی در سطح سرور شود. به همین منظور، کسانی که در حوزه امنیت SQL Server فعالیت می‌کنند، باید با انواع Server Role ها آشنایی داشته باشند تا بتوانند از عهده چالش‌های امنیتی SQL Server در سازمان‌های خود برآیند.

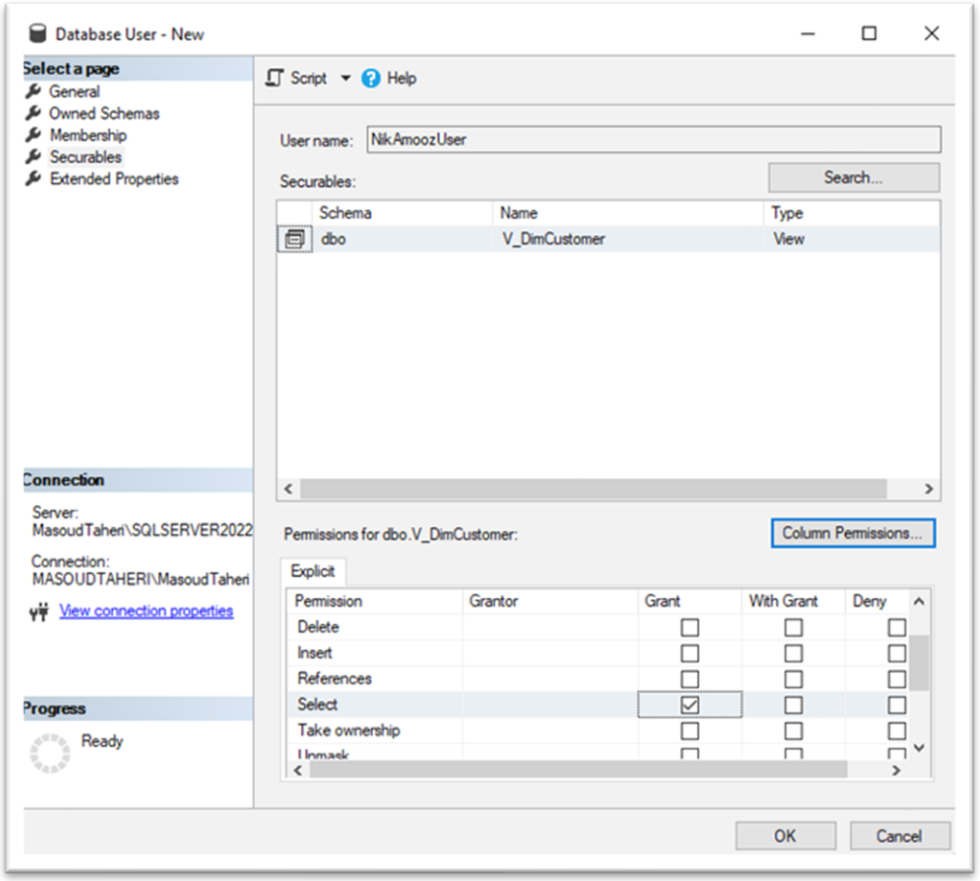


بخش پانزدهم: بررسی User

- بررسی نحوه اعطای مجوز به کاربران
- بررسی نحوه گرفتن مجوز از کاربران
- بررسی دستورات Grant، Revoke، Deny
- بررسی سناریوهای کاربردی درخصوص تخصیص دسترسی به User ها
- بررسی نحوه Impersonate کردن به دسترسی یک User
- بررسی Database Permission های جدید در نسخه جدید SQL Server

- بررسی Ownership Chains
- بررسی نحوه تعریف کاربر با کمترین دسترسی برای کار با اشیاء بانک اطلاعاتی
- بررسی توابع ، DMF، DMV و SP های مربوط به این حوزه

اگر بخواهید اشیاء مربوط به یک بانک اطلاعاتی را محدود کرده و درگیر دسترسی و... نمائید، باید از User های موجود در Database کمک بگیرید. ما در SQL Server می‌توانیم کارهای جالبی با استفاده از User ها انجام دهیم. برای مثال، می‌توانیم یک User داشته باشیم که صرفاً بتواند از داده‌های موجود در یک ویو Select بگیرد. استفاده از این موضوع می‌تواند برای امنیت سرورهای شما مفید واقع شود.

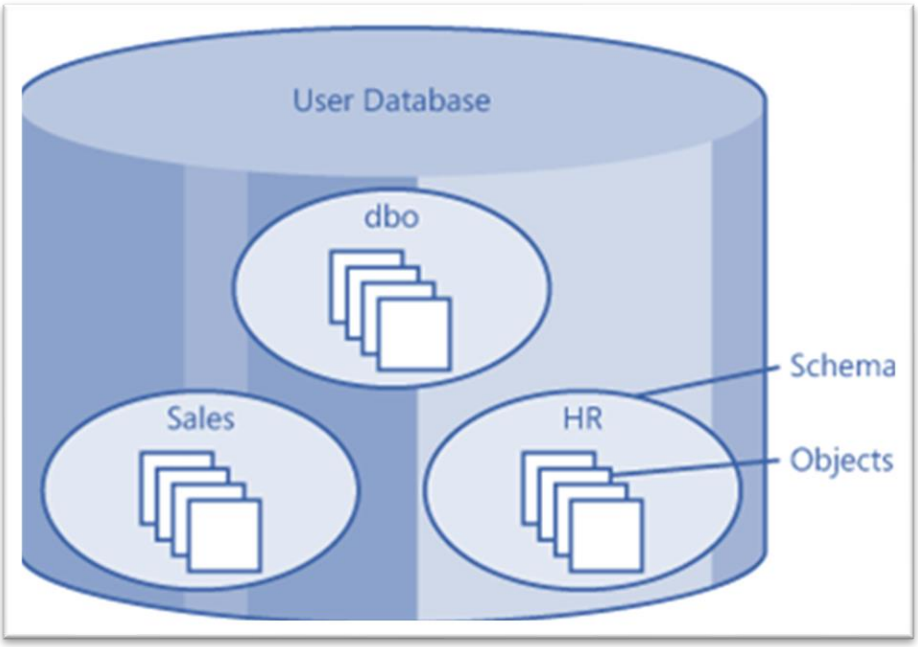


بخش شانزدهم: بررسی Schema در SQL Server

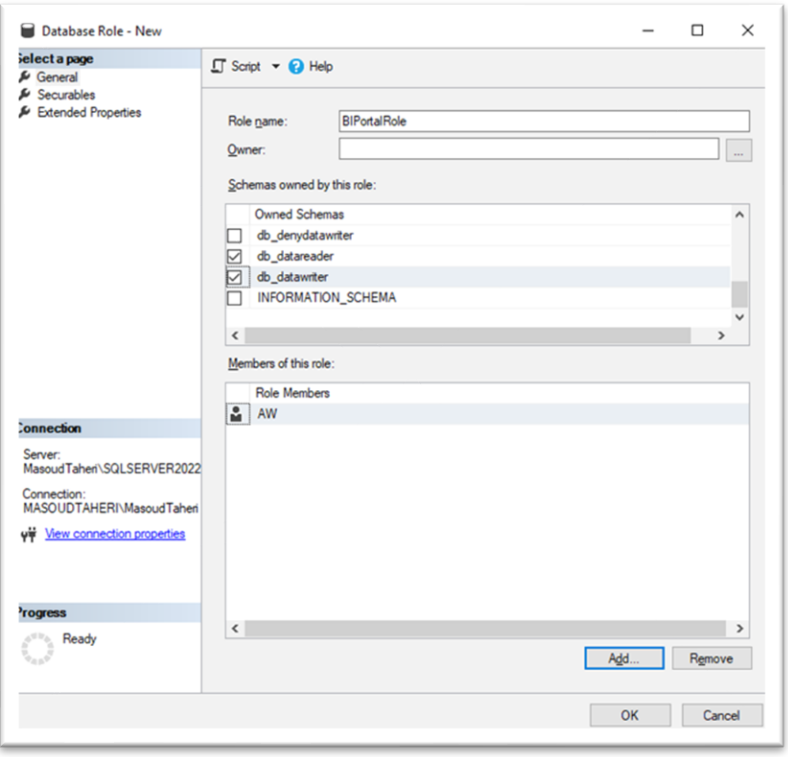
- بررسی مفهوم Schema
- بررسی نحوه ایجاد Schema
- بررسی نحوه قراردادن اشیاء (جدول، ویو و...) در Schema
- بررسی نحوه کنترل دسترسی و امنیت با استفاده از Schema
- بررسی نحوه تغییر Schema
- بررسی نحوه حذف کردن Schema

مدرس: مسعود طاهری

استفاده از Schema در SQL Server برای اولین بار در SQL Server ۲۰۰۵ به‌وجود آمد. با استفاده از این ویژگی، می‌توانیم اشیاء موجود در بانک اطلاعاتی را گروه‌بندی کرده و امنیت مربوط به آن‌ها را تأمین نمائیم. ما در طی این دوره به شما در این خصوص تکنیک‌های کاربردی را آموزش خواهیم داد.



بخش هفدهم: بررسی Database Role



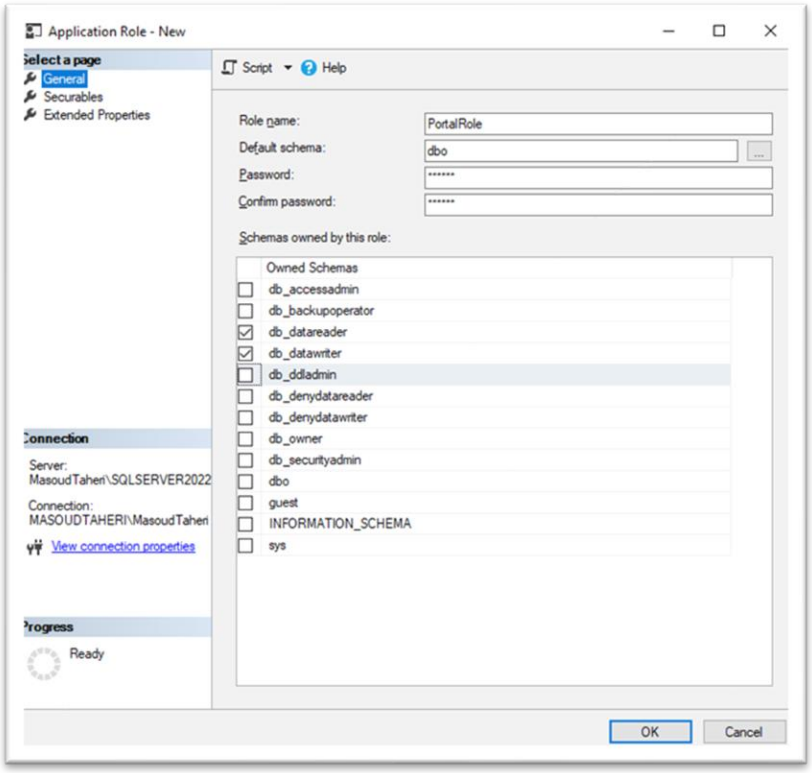
- معرفی مفهوم Role و انواع آن
- بررسی Database Role
- بررسی انواع Database Role ها در SQL Server
- بررسی نحوه ایجاد Database Role ها سفارشی در SQL Server
- اعمال دسترسی سفارشی به ازای Role های سفارشی
- بررسی DMV های مربوط به Database Role ها

یکی از امکانات جالب SQL Server در سطح بانک اطلاعاتی، Database Role ها هستند. شاید شنیده باشید که خیلی از دوستان برای دسترسی Application های خود به بانک اطلاعاتی یک Login تعریف کرده و متناسب با آن، یک User تعریف کرده و نقش آن را db_owner بانک اطلاعاتی قرار می‌دهند. این موضوع می‌تواند از لحاظ امنیتی کمی خطرناک باشد؛ به دلیلی این لاگین Application شما دسترسی فراتر از بحث خواندن و نوشتن داده‌ها در جداول دارد. برای مثال، با استفاده از دسترسی db_owner برنامه شما می‌تواند جداول، ایندکس‌ها و... را به‌راحتی حذف نماید. به همین منظور، پیشنهاد ما این است که شما Database Role های سفارشی ایجاد کرده و دسترسی به بانک اطلاعاتی خود را با استفاده از این موضوع کنترل نمایید.

بخش هجدهم: بررسی Application Role

- بررسی مفهوم Application Role ها
- بررسی نحوه ایجاد Application Role ها
- بررسی کاربرد Application Role ها
- بررسی نحوه تخصیص دسترسی به Application Role ها
- بررسی نحوه کار با پروسیجر sp_setapprole هنگام کار با Application Role ها
- بررسی DMV های مربوط به Application Role ها

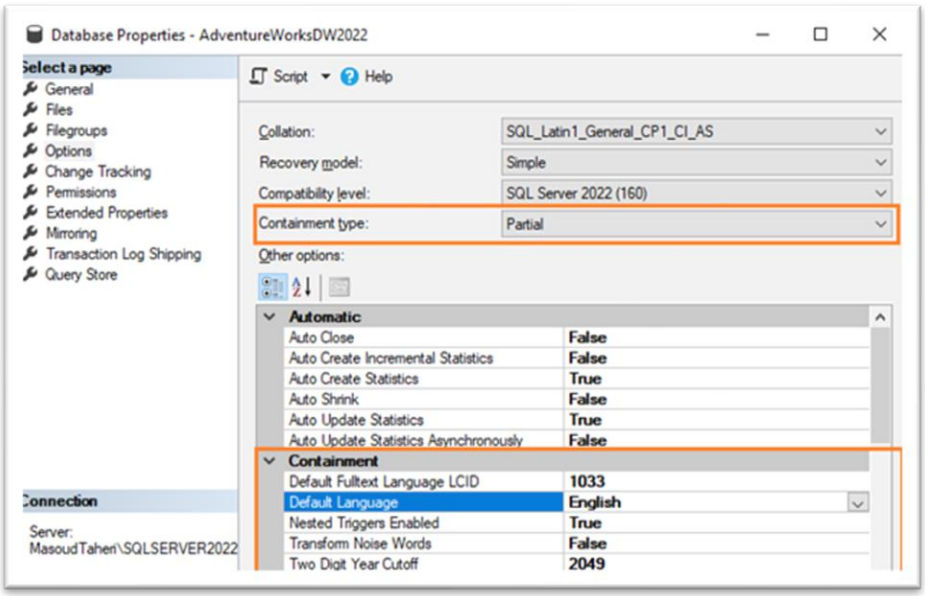
لاگین Application کاربردی شما بنا به دلایلی در دسترس برخی از افراد است. انتظار شما این است که این لاگین مخصوص Application باشد و کاربری نتواند با برنامه‌ای دیگر مثل SSMS و... به بانک اطلاعاتی وصل شود. برای این منظور اگر بخواهید که دسترسی این لاگین صرفاً به دیتابیس موردنظر شما با استفاده از Application خودتان باشد، باید از Application Role ها استفاده نمایید. ما در طی این دوره، نحوه استفاده از این موضوع را به شما آموزش خواهیم داد.



بخش نوزدهم: بررسی Contained Database

- بررسی Contained Database
- بررسی تنظیمات مربوط به Contained Database Authentication
- بررسی تنظیمات Containment Type در Database
- بررسی نحوه ایجاد SQL User با Password
- بررسی نحوه اتصال به پایگاه داده‌ای که قابلیت Contained Database را پشتیبانی می‌کند
- بررسی DMV و DMF های وابسته به مبحث Contained Database

شرکت ما یک نرم‌افزار کاربردی ایجاد کرده که بانک اطلاعاتی آن SQL Server است و برای نصب آن در سازمان‌ها درگیر ایجاد مباحثی مانند Login و... می‌باشد، ما دنبال این موضوع هستیم که صرفاً Backup بانک اطلاعاتی خودمان را بر روی سرور مشتری راه‌اندازی کرده و همه مباحث مربوط به Login و دسترسی داخل خود بانک اطلاعاتی باشد. در SQL Server این موضوع را می‌توانیم با استفاده از Contained Database رفع و رجوع نماییم.



بخش بیستم: بررسی Database Snapshot و نکات امنیتی آن

- معرفی Database Snapshot
- بررسی کاربردهای Database Snapshot
- بررسی نحوه تنظیم Database Snapshot بر روی بانک اطلاعاتی
- بررسی تاثیر استفاده از Database Snapshot بر روی امنیت بانک‌های اطلاعاتی
- بررسی محدودیت‌های Database Snapshot

مدرس: مسعود طاهری

یکی از ویژگی‌های جالب SQL Server که می‌تواند برای تهیه کپی لحظه از وضعیت حال حاضر یک بانک اطلاعاتی مورد استفاده قرار گیرد، Database Snapshot (تصویر لحظه‌ای) است. این موضوع می‌تواند در سناریوهایی امنیتی بانک‌های اطلاعاتی مورد استفاده قرار گیرد. استفاده این موضوع برای تیم ما در یک از پروژه‌هایی که داشتیم، کاربردی بوده است. در طی این پروژه، ما نیاز داشتیم که Snapshot کلیه داده‌های بانک اطلاعاتی را سه بار در طی روز داشته باشیم تا بتوانیم روند تغییر داده‌ها را طی آن فواصل زمانی بررسی داشته باشیم.

بخش بیست و یکم: بررسی Linked Servers و نکات امنیتی آن

- آموزش نحوه راه‌اندازی Linked Servers جهت اتصال به سایر Instance ها
- بررسی تنظیمات امنیتی در Linked Server
- پیاده‌سازی Impersonation در Linked Server
- استفاده از Synonym هنگام کار با Linked Server
- آشنایی با مفهوم Distributed Query و نحوه پیاده‌سازی آن در SQL Server

در سازمان‌هایی که با آن‌ها کار کرده‌ام، برخی از Application ها از Linked Server برای ارتباط مابین سرورهای خود استفاده می‌کنند. زمانی که به تنظیمات امنیتی مربوط به Linked Server مراجعه می‌کنم، با کمال تعجب مشاهده می‌کنم که کلیه کارها با دسترسی Full Access به سرور مقصد انجام می‌شود و هیچ کنترلی برروی آن وجود ندارد. زمانی که دلیل این موضوع را جویا می‌شویم، با کمال تعجب این جواب را می‌شنویم که برای راحتی کار و همچنین نیاز برنامه، در صورتی که که اگر بررسی دقیق انجام دهید، متوجه می‌شوید که برنامه اصلاً نیاز به چنین دسترسی سمت Linked Server نداشته و با دسترسی محدود می‌توان کار را انجام داد.

بخش بیست و دوم: بررسی PolyBase و نکات امنیتی مربوط به آن

- بررسی Polybase و کاربرد آن در SQL Server
- بررسی نحوه نصب و راه‌اندازی PolyBase
- بررسی مفهوم External Table در SQL Server
- بررسی استفاده از Polybase جهت اتصال به سایر بانک‌های اطلاعاتی
- بررسی نتظیمات امنیتی برای کار با PolyBase
- مقایسه PolyBase و Linked Server

اگر دنبال اتصال راحت SQL Server به سایر بانک‌های اطلاعاتی مانند Oracle، MongoDB و... هستید، می‌توانید از PolyBase برای این موضوع کمک بگیرید. برای کار، با این تکنولوژی باید با ویژگی‌های امنیتی آن آشنا باشید تا بتوانید در محیط‌های عملیاتی، به بهترین نحو ممکن از آن استفاده نمایید.

بخش بیست و سوم: ایجاد Function ها و نکات امنیتی مربوط به آن

- بررسی نکات امنیتی مناسب برای کار با Function ها
- بررسی انواع Permission های لازم در سطح Database برای کار با Function ها
- بررسی DMV های مفید برای کار با Function ها
- بررسی نحوه Encrypt کردن سورس Function ها
- بررسی نحوه برگرداندن سورس Function های Encrypt شده

بخش بیست و چهارم: ایجاد Stored Procedure ها و نکات امنیتی مربوط به آن

- بررسی نکات امنیتی مناسب برای کار با Stored Procedure ها
- بررسی انواع Permission های لازم در سطح Database برای کار با Stored Procedure ها
- بررسی DMV های مفید برای کار با Stored Procedure ها
- بررسی نحوه Encrypt کردن سورس Stored Procedure ها
- بررسی نحوه برگرداندن سورس Stored Procedure های Encrypt شده

بخش بیست و پنجم: معرفی Procedure ها و Function های پرکاربرد و نکات امنیتی مربوط به آن‌ها

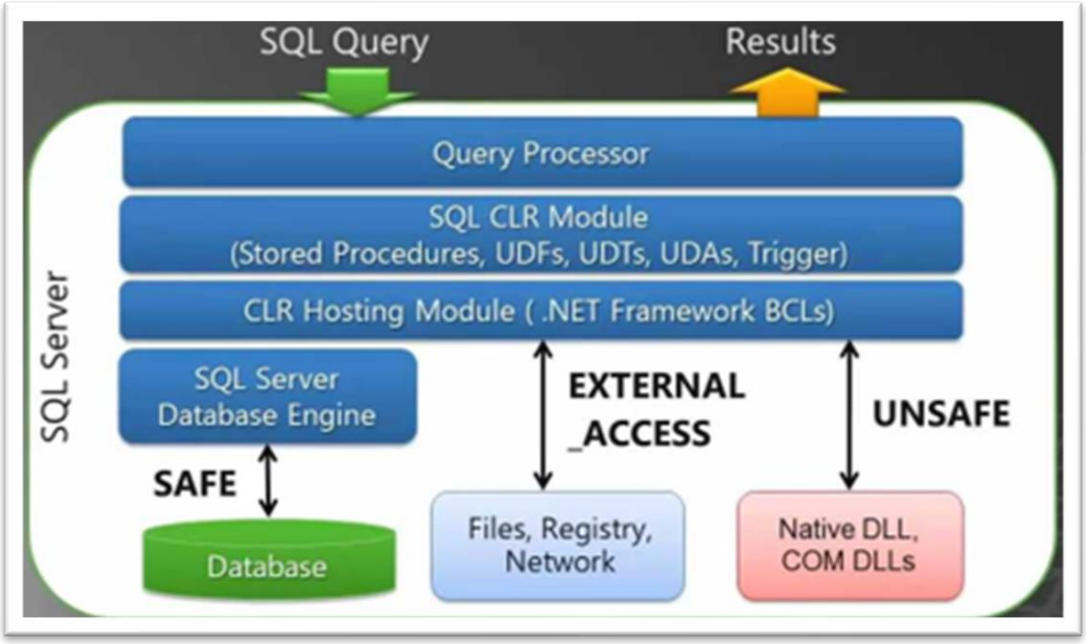
- بررسی پروسیجر سیستمی sp_ExecuteSQL
- بررسی پروسیجر سیستمی xp_cmdshell
- بررسی پروسیجر سیستمی sp_execute_external_script
- بررسی تابع OpenRowSet
- پیکربندی SQL Server جهت اجرای OS Command
- بررسی ریسک‌های فعال بودن قابلیت اجرای OS Commands برروی SQL Server

مدرس: مسعود طاهری

بخش بیست و ششم: استفاده از CLR و نکات امنیتی مربوط به آن

- CLR چیست؟
- بررسی تنظیمات SQL Server برای کار با CLR
- بررسی انواع CLR Object های قابل استفاده برای SQL Server
- نحوه ایجاد Function های CLR و Register کردن آن‌ها در .NET
- بررسی سطوح امنیتی هنگام کار با CLR در SQL Server
- بررسی استخراج سورس CLR Object های از SQL Server

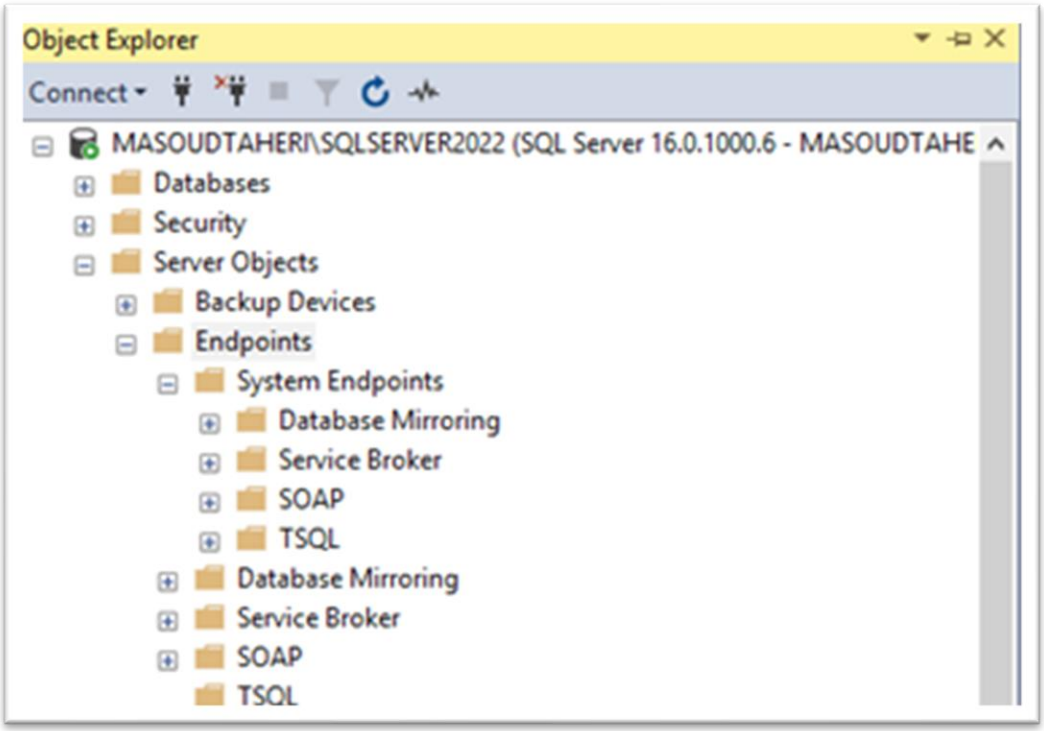
استفاده از اشیاء CLR مانند پروسیجر، توابع، تریگر و... در بانک‌های اطلاعاتی جدید، میان توسعه‌گران باب شده است. زمانی که شما از CLR استفاده می‌کنید، می‌توان سطوح امنیتی مربوط به آن را هنگام Register کردن اسمبلی‌ها در SQL Server مشخص کنید. این تنظیم توسط خیلی از دوستان نادیده گرفته شده و در برخی از موارد برای راحتی کار و جلوگیری از خطا و... ، عموماً به‌صورت Unsafe درنظر گرفته می‌شود که این موضوع می‌تواند باعث به‌وجود آمدن مشکلات امنیتی در شرایطی خاص شود.



بخش بیست و هفتم: بررسی Endpoint و نکات امنیتی مربوط به آن

- بررسی Endpoint و کاربرد آن در SQL Server
- بررسی انواع Endpoint ها و کاربرد هرکدام از آن‌ها
- اعمال امنیت برروی Endpoint ها
- بررسی DMV های مرتبط با Endpoint ها

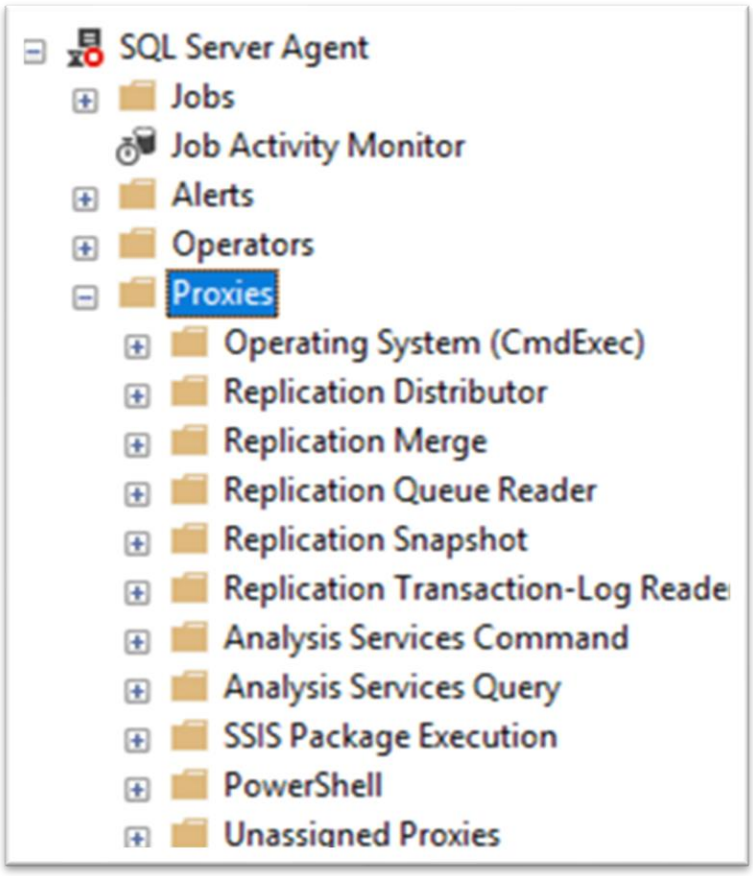
در SQL Server تمامی تعاملات شبکه با استفاده از Endpoint در SQL Server انجام می‌شود. نقطه پایانی یا Endpoint ، یک اصطلاح کلی برای نقطه اتصال بین یک کلاینت و یا سرور شبکه است که با تنظیم مناسب آن هنگام استفاده از تکنولوژی‌هایی مانند Service Broker، Database Mirroring و...، امنیت سرورها را تضمین می‌کند. ما در طی این دوره، نحوه ایجاد Endpoint و تنظیمات امنیتی مربوط به آن‌ها را یاد خواهیم گرفت.



بخش بیست و هشتم: بررسی استفاده از Proxy برای پیاده‌سازی امنیت

- بررسی مفهوم Proxy و سناریوهای استفاده از آن
- بررسی انواع Proxy در SQL Server
- بررسی مفهوم Credential برای کار با Proxy
- استفاده از Proxy برای پیاده‌سازی سناریوهای امنیتی

در برخی مواقع لازم است که شما دستورات Power Shell را در SQL Server اجرا نمایید. برای این منظور، باید اکانتی که سرویس SQL Server به‌وسیله آن استارت زده شده است، توانایی اجرای دستور Power Shell موردنظر را داشته باشد؛ اما این موضوع از لحاظ امنیتی صحیح نیست. راهکار اصولی برای این منظور، استفاده از Proxy است که با استفاده از آن می‌توانیم عملیات Impersonation (جعل هویت) را انجام دهیم. در این حالت، زمانی که می‌خواهیم دستور Power Shell را اجرا نماییم، هویت خود را تغییر داده (جعل) و با دسترسی یک کاربر سطح بالا کار موردنظر را انجام دهیم.



بخش بیست و نهم: بررسی SQL Injection

- SQL Injection چیست؟
- بررسی نحوه Inject کردن دستورات TSQL به یک Application
- بررسی تکنیک‌های کاربردی جهت جلوگیری از SQL Injection

هنوز که هنوز است SQL Injection یکی از بیشترین روش‌های هک‌کردن بانک‌های اطلاعاتی است. یادم است چند سال پیش یکی از دوستان، یک Windows App برای سازمانی ایجاد کرده بود. به خاطر اینکه ضعف امنیتی مربوط به Application را به او گوشزد کنم، به‌راحتی آب خوردن با استفاده از SQL Injection توانستم دسترسی Remote بگیرم؛ توجه داشته باشید دسترسی Remote به سرور.

بخش سی‌ام: بررسی Encryption در SQL Server

- بررسی دلایل Encrypt و Decrypt کردن داده‌ها در SQL Server
- بررسی مفهوم Hash و پیاده‌سازی آن در SQL Server
- مقایسه نتیجه الگوریتم‌های Hash مربوط به SQL Server و .NET
- بررسی Service Master Key
- بررسی Database Master key
- بررسی Symmetric Key و نحوه استفاده از آن برای Encrypt کردن Data
- بررسی Asymmetric Key و نحوه استفاده از آن برای Encrypt کردن Data
- بررسی مفهوم Certificate و رمزگذاری دیتا با استفاده از Certificate
- محافظت ار داده‌ها توسط امضاء دیجیتالی
- بررسی سلسه‌مراتب Encryption در SQL Server
- بررسی Authenticating stored procedure by signature
- بررسی Extensible Key Management
- بررسی توابع، DMF، DMV وSP های مربوط به این حوزه

چند سال پیش در یکی از سازمان‌های دولتی به‌صورت مشاوره‌ای درگیر پروژه‌ای بودم، یکی از جداول بانک اطلاعاتی داده‌های بسیار حساسی داشت. برنامه‌نویسان این سازمان دنبال روشی بودن که بتواند از داده‌های این جدول محافظت کنند؛ به‌طوری که اگر بیتی از اطلاعات این جدول توسط شخص یا برنامه دیگری به جزء برنامه اصلی تغییر پیدا کرد، رکورد موردنظر اعتبار نداشته باشد. روشی که برای این منظور ما استفاده کردیم، محافظت داده‌ها توسط Certificate یا امضاء دیجیتالی در SQL Server بود.

بخش سی و یکم: استفاده از TDE در بانک‌های اطلاعاتی

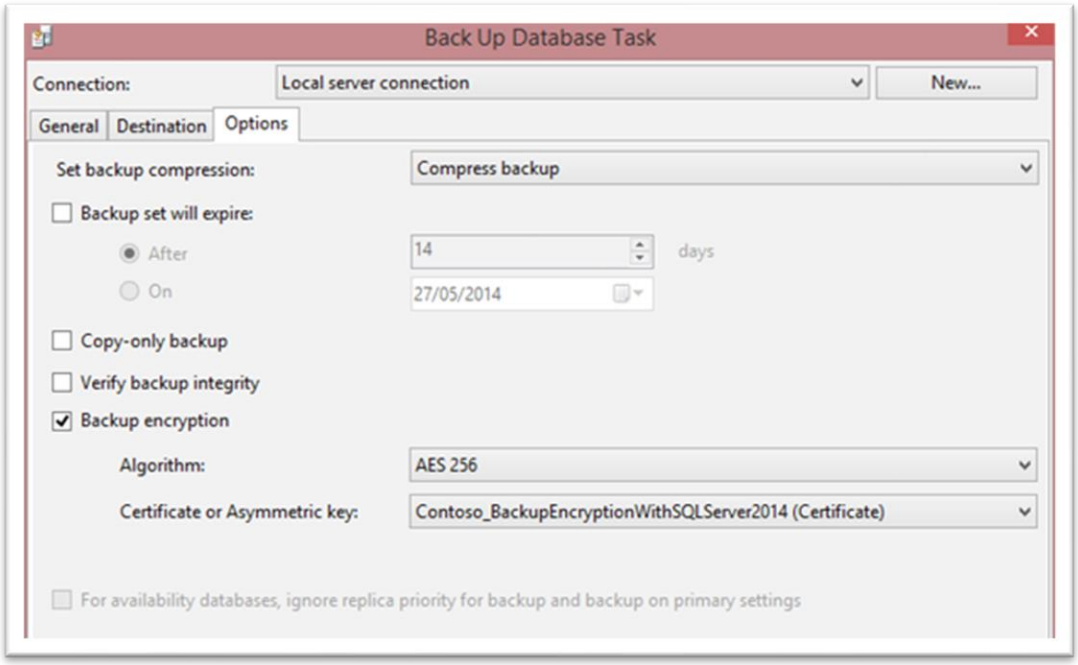
- معرفی Transparent Database Encryption
- بررسی نحوه استفاده از TDE در SQL Server
- بررسی پیاده‌سازی اصولی TDE به ازای بانک‌هایی
- بررسی نحوه تهیه نسخه پشتیبان از کلیدهای مورد استفاده از جهت عملیات Encrypt و Decrypt
- بررسی مزایا و معایب استفاده از TDE
- بررسی تأثیر استفاده از TDE بر کارایی بانک اطلاعاتی
- بررسی تأثیر استفاده از TDE برروی بانک‌های اطلاعاتی سیستمی
- بررسی تأثیر استفاده از TDE در Log File, Data File, Backup File
- بازیابی بانک اطلاعاتی که با TDE رمزگذاری‌شده در یک سرور دیگر

یکی از شرکت‌های خصوصی که با آن کار می‌کردم، به دنبال روشی برای جلوگیری از سرقت فایل‌های فیزیکی بانک اطلاعاتی بود. مسئله از اینجا شروع شده بود که شرکت متوجه شده بود که نسخه‌ای از بانک اطلاعاتی مربوط به آن در سازمانی دیگر مورد استفاده قرار گرفته است. پس از بررسی، مشخص شد که ادمین سیستم با Stop کردن سرویس SQL Server و کپی کردن Data File و Log File بانک اطلاعاتی، آن را به سازمان دیگر منتقل کرده و مورد استفاده قرار داده است. ما برای اینکه این فرآیند را مشکل کنیم (جلوی آن را بگیریم)، از TDE استفاده کردیم.

بخش سی و دوم: بررسی امنیت نسخه‌های پشتیبان در SQL Server

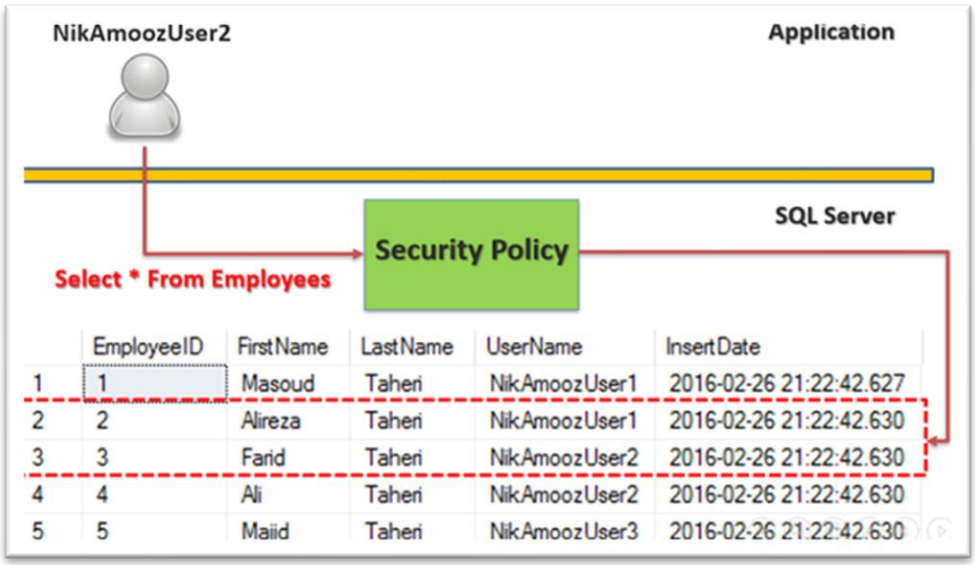
- بررسی تنظیمات اولیه لازم برای Encrypt کردن نسخه پشتیبان
- بررسی الگوریتم‌های پشتیبانی‌شده برای Encryption نسخه پشتیبان
- بررسی نحوه تهیه نسخه پشتیبان به روش Encrypt
- بررسی نحوه Restore کردن نسخه پشتیبان Encrypt شده
- بررسی نحوه استفاده از Maintenance Plan برای تهیه نسخه پشتیبان به‌صورت Encrypt

یکی از سؤالاتی که از من زیاد پرسیده می‌شود، این است آیا ما می‌توانیم در SQL Server نسخه پشتیبان خود را Encrypt کنیم؛ به‌طوری که روی هر سرور به‌راحتی قابل بازیابی نباشد؟ پاسخ این سؤال، بلی است؛ شما در SQL Server می‌توانید با استفاده از امکانات آن نسخه پشتیبان خود را Encrypt کنید.



بخش سی و سوم: استفاده از Row Level Security

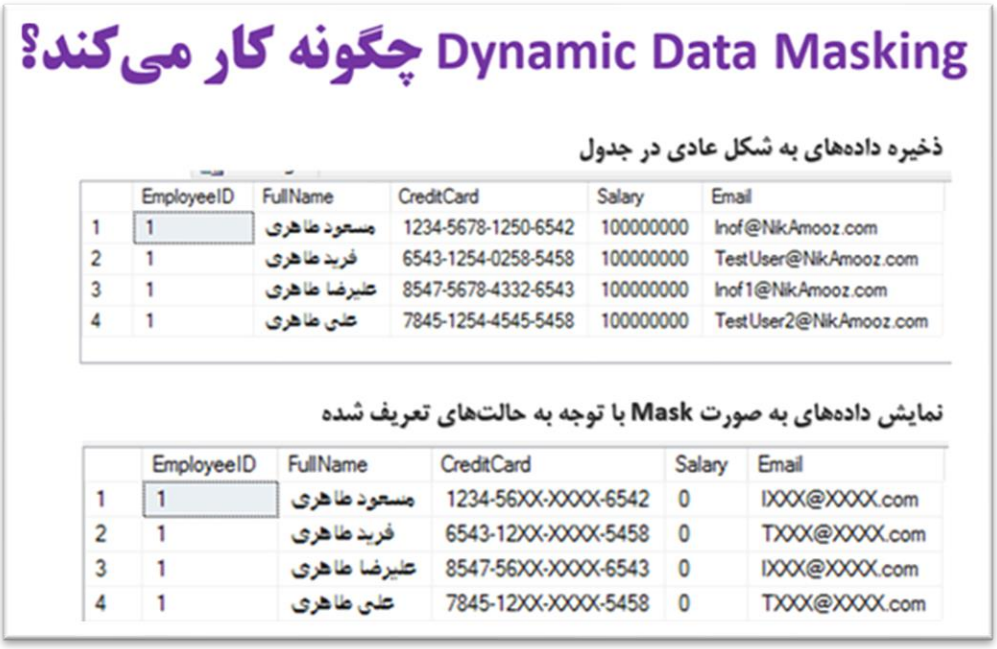
- بررسی تأثیر استفاده از RLS برای پیاده‌سازی امنیت در SQL Server
- بررسی نحوه اعمال RLS برروی جداول
- بررسی نحوه تنظیم Security Policy برای کار با RLS
- بررسی Security Predicate
- پیاده‌سازی Row Level Security با استفاده دات نت



اهمیت داده‌های حساس در سازمان‌ها برای همه روشن است. مخصوصاً زمانی که در بانک اطلاعاتی شما رکوردهایی وجود داشته باشد که نمایش آن‌ها برای همه ممکن نباشد. اگر بخواهیم چنین سناریوی را پیاده‌سازی کنیم، قطعاً مجبور هستیم همیشه دسترسی رکورد موردنظر را برای همه کاربران (Business User) چک کنیم. با هر روشی که فکر می‌کنید و این موضوع، یعنی تغییرات گسترده سمت Application و Database. اما در SQL Server شما می‌توانید با استفاده از Row Level Security با انجام حداقل تغییرات سمت بانک Application و Database این کار را انجام دهید.

بخش سی و چهارم: استفاده از Dynamic Data Masking

- بررسی تأثیر استفاده از Dynamic Data Masking برای پیاده‌سازی امنیت در SQL Server
- بررسی نحوه اعمال Dynamic Data Masking برروی جداول
- بررسی انواع توابع مربوط به Mask کردن داده‌ها
- پیاده‌سازی Dynamic Data Masking با استفاده دات نت



	EmployeeID	FullName	CreditCard	Salary	Email
1	1	مسعود طاهری	1234-5678-1250-6542	100000000	Inof@NikAmooz.com
2	1	فرید طاهری	6543-1254-0258-5458	100000000	TestUser@NikAmooz.com
3	1	علیرضا طاهری	8547-5678-4332-6543	100000000	Inof1@NikAmooz.com
4	1	علی طاهری	7845-1254-4545-5458	100000000	TestUser2@NikAmooz.com

	EmployeeID	FullName	CreditCard	Salary	Email
1	1	مسعود طاهری	1234-56XX-XXXX-6542	0	IXXX@XXXX.com
2	1	فرید طاهری	6543-12XX-XXXX-5458	0	TXXX@XXXX.com
3	1	علیرضا طاهری	8547-56XX-XXXX-6543	0	IXXX@XXXX.com
4	1	علی طاهری	7845-12XX-XXXX-5458	0	TXXX@XXXX.com

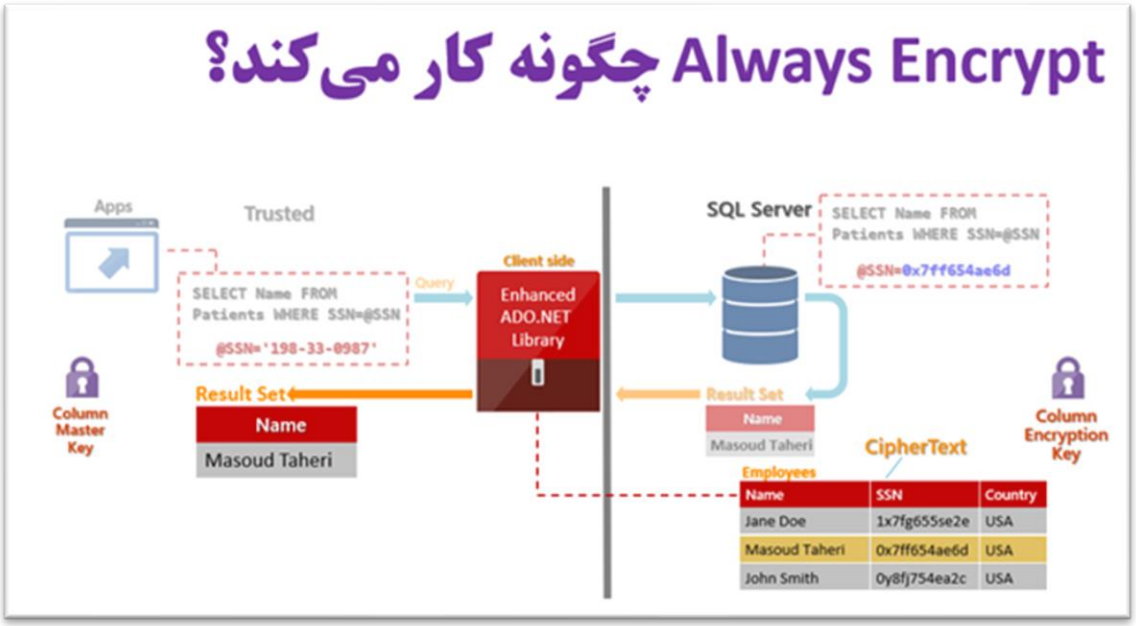
یادم می‌آید زمانی که در یک مجموعه بزرگ بانکی کار می‌کردم که نسخه SQL Server آن‌ها ۲۰۰۸ SQL Server و ۲۰۱۲ SQL Server بود. یکی از مواردی که این مجموعه دنبال آن بود، نمایش داده‌های حساس (مثل مبلغ تراکنش، شماره کارت و...) به‌صورت Mask شده بود، انجام این کار در سطح Application به سختی و با تغییرات زیادی همراه بود. زمانی که SQL Server ۲۰۱۶ ارائه شد و ویژگی Dynamic Data Masking ارائه شد، یاد مشکلات و سختی‌های پروژه قبلی خودم افتادم و با خودم می‌گفتم ای کاش این ویژگی، چندسال زودتر ارائه شده بو

مدرس: مسعود طاهری

بخش سی و پنجم: استفاده از Always Encrypt

- بررسی تأثیر استفاده از Always Encrypt برای پیاده‌سازی امنیت در SQL Server
- بررسی نحوه اعمال Always Encrypt برروی فیلدهای جداول
- بررسی Column Master Key
- بررسی Column Encryption Key
- بررسی تغییر کلید در هنگام استفاده از Always Encrypt
- بررسی محدودیت‌های Always Encrypt
- پیاده‌سازی Always Encrypt با استفاده دات نت

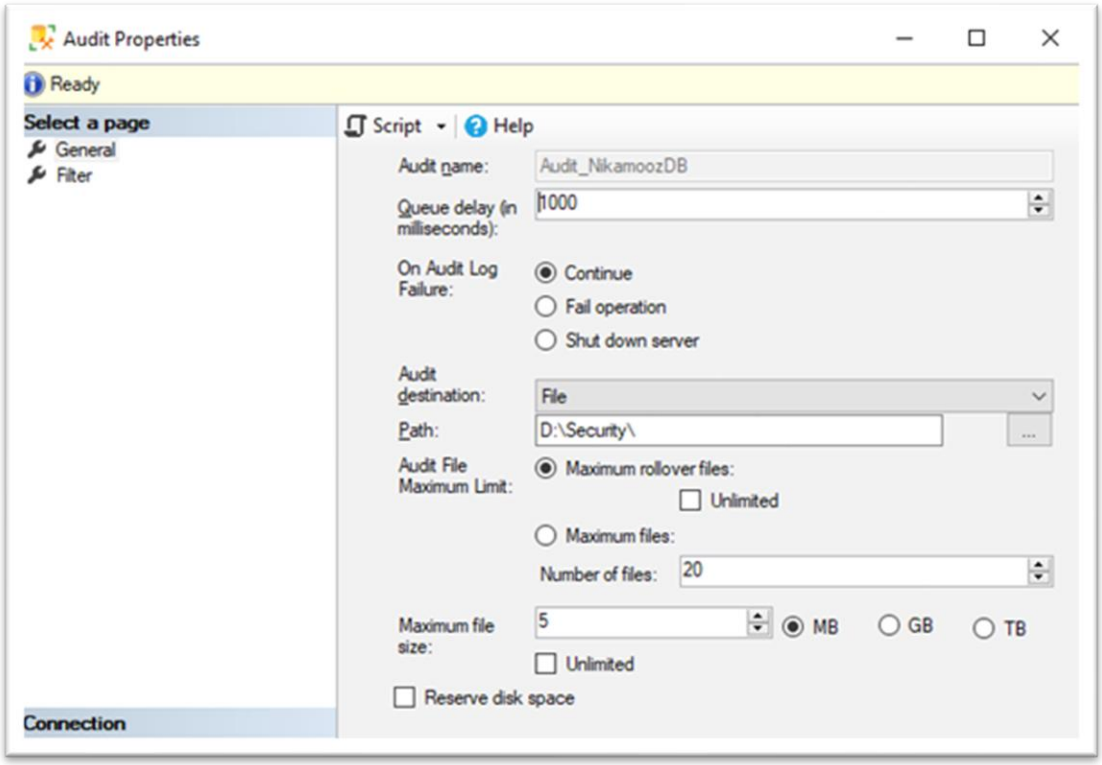
یکی از مجموعه‌های دولتی که با آن درحال کار هستم، داده‌های حساس در یکی از جداول خود داشت که دنبال Encrypt کردن آن به ساده‌ترین روش ممکن با دردسر کمتر بود. راهکار باید طوری باشد که حتی ادمین سیستم هم نتواند داده‌ها را به‌صورت Decrypt شده مشاهده نماید؛ مگر با داشتن کلید Decryption . برای این منظور در SQL Server ویژگی Always Encrypt وجود دارد که به‌وسیله آن می‌توان داده‌ها را به‌صورت خودکار Encrypt و Decrypt کرد. با استفاده از این ویژگی می‌توان کمترین میزان تغییر در سمت Application و همچنین بانک اطلاعاتی را خواهید داشت و هرکجا شما Certificate لازم عملیات Decrypt و Encrypt براساس آن و کتابخانه‌های موجود در Application شما انجام خواهد شد.



بخش سی و ششم: استفاده از Audit جهت پیاده‌سازی امنیت در SQL Server

- بررسی مفهوم Audit
- بررسی نحوه پیکربندی Audit ها در SQL Server
- بررسی نحوه پیکربندی Server Audit Specification
- بررسی نحوه پیکربندی Database Audit Specification
- بررسی نحوه تعریف Audit های سفارشی در SQL Server
- معرفی DMV ها و DMF ها مربوط به کار با Audit ها در SQL Server
- بررسی نحوه خواندن محتوای Audit File ها و انتقال آن به جداول
- بررسی نحوه پیاده‌سازی Login Audit
- بررسی نحوه پیاده‌سازی C2 Audit

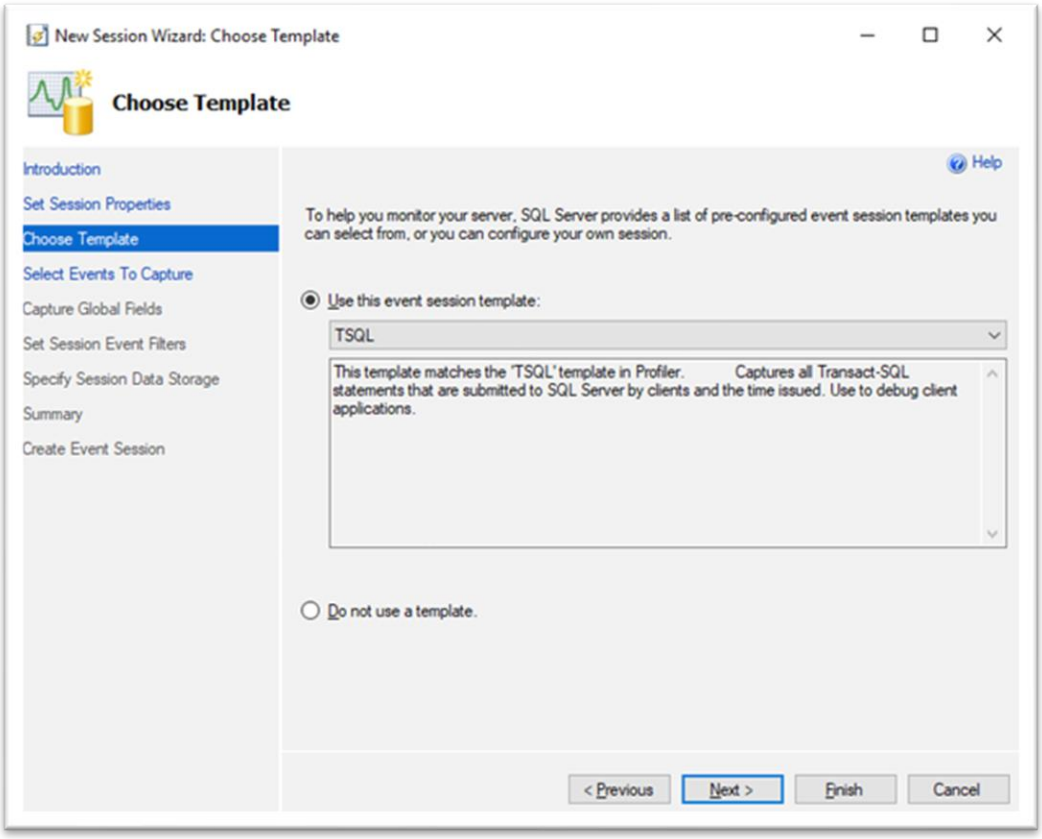
ما می‌خواهیم کلیه دستوراتی که برروی تعدادی از جدول خاص اجرا می‌شود را جمع‌آوری کنیم. این سؤالی است که خیلی‌ها از من می‌پرسند. برای این موضوع، می‌توانیم از ویژگی Audit در SQL Server استفاده نمائیم.



بخش سی و هفتم: استفاده از Extended Events ها جهت پیاده‌سازی امنیت در SQL Server

- بررسی پیکربندی Extended Events
- بررسی مفهوم Session در Extended Events
- بررسی مفهوم Action در Extended Events
- بررسی مفهوم Filter در Extended Events
- بررسی مفهوم Target در Extended Events
- پیاده‌سناریو جمع‌آوری کوئری‌های ارسالی به SQL Server
- پیاده‌سازی سناریو نحوه کشف دستورات ارسالی توسط Business User به سمت SQL Server
- بررسی نحوه خواندن محتوای فایل‌های Extended Events و انتقال آن به جداول

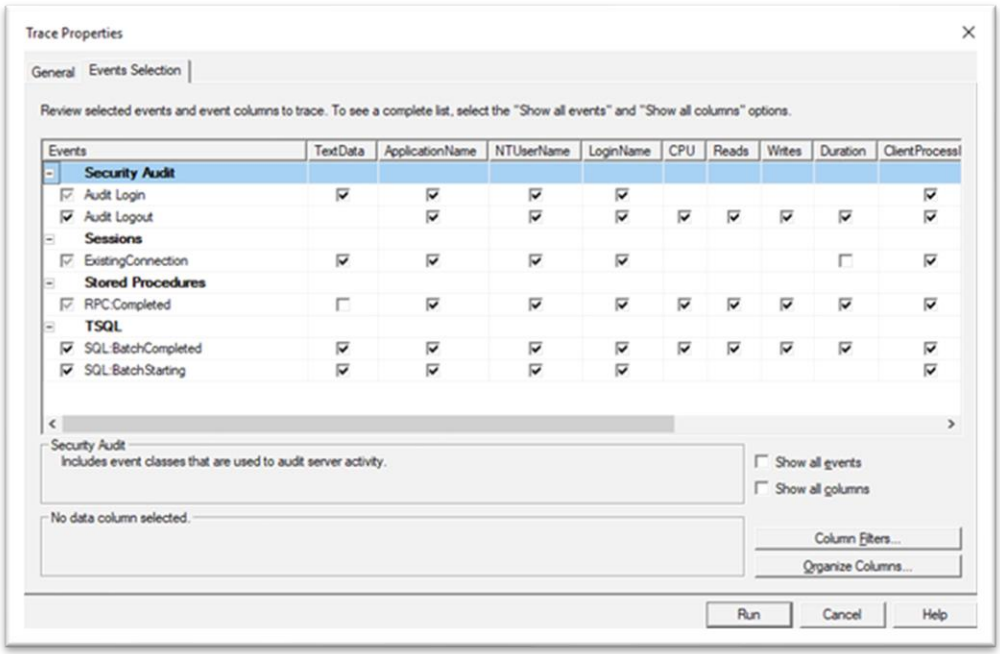
یکی دیگر از راهکارهای پیاده‌سازی Audit در SQL Server ، استفاده از Extended Event است. ما در SQL Server می‌توانیم با انجام تنظیمات پیشرفته به ازای Extended Event ها، لاگ‌های مفیدی از عملکرد کاربران در سطح SQL Server جمع‌آوری کنیم.



بخش سی و هشتم: استفاده از SQL Server Profiler جهت پیاده‌سازی امنیت در SQL Server

- معرفی برنامه SQL Server Profiler
- بررسی مفاهیم Event، Filer، Template و...
- بررسی Event های امنیتی در SQL Server Profiler
- بررسی نحوه راه‌اندازی Trace ها به‌صورت همیشگی
- بررسی نحوه راه‌اندازی Trace های Server Side برای جمع‌آوری لاگ‌های امنیتی
- بررسی نحوه خواندن محتوای فایل‌های Trace و انتقال آن به جداول

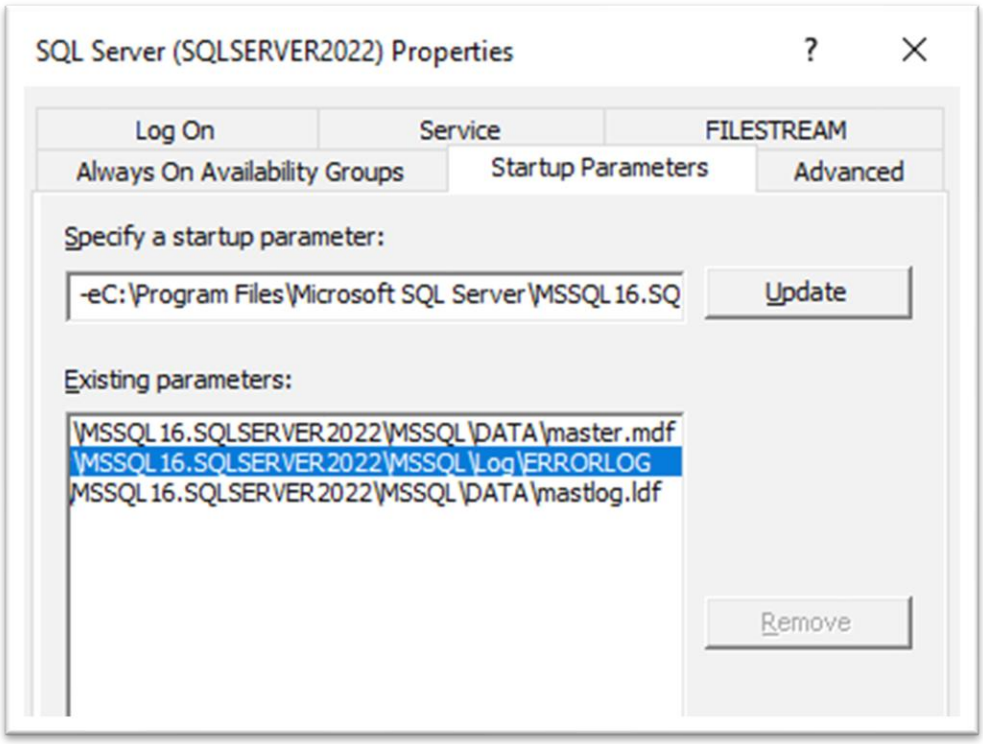
شاید باورتان نشود اما یکی از روش‌های رایج راه‌اندازی Audit در SQL Server ، استفاده از Trace های Server Side است. در SQL Server برای پیاده‌سازی این ویژگی می‌توانیم از SQL Server Profiler استفاده کنیم.



بخش سی و نهم: استفاده از SQL Server Error Logs برای بررسی موارد امنیتی

- بررسی نحوه کار با SQL Server Logs
- بررسی نحوه استفاده از پروسیجرهای بررسی Log
- بررسی نحوه پیکربندی اصولی SQL Server Error Logs
- بررسی نحوه استخراج Log های امنیتی ثبت‌شده در نرم‌افزار

یکی از بخش‌های که لاگ‌های امنیتی SQL Server در آن جمع می‌شود، SQL Server Logs است. تنظیمات مربوط به این بخش از اهمیت زیادی برخوردار است. ما همواره توصیه می‌کنیم که محل قرارگیری لاگ‌ها را به‌صورت مناسب تنظیم نمایید.



بخش چهلم: استفاده از Trigger ها جهت پیاده‌سازی امنیت در SQL Server

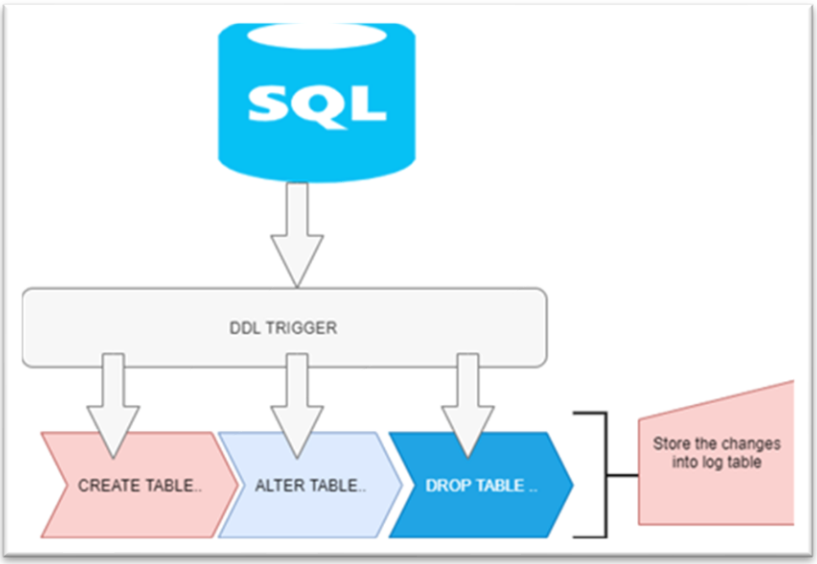
- بررسی تریگرها در SQL Server
- بررسی After Trigger ها و کاربرد آن در امنیت
- بررسی Instead of Trigger ها و کاربرد آن در امنیت
- بررسی Logon Trigger و کاربرد آن در امنیت
- بررسی DDL Trigger ها و کاربرد آن در امنیت
- پیاده‌سازی سناریو جمع‌آوری تغییرات مربوط به ساختار اشیاء در SQL Server
- پیاده‌سازی سناریوهای ثبت تغییرات رکوردها با استفاده از تریگرها

این سؤال شاید در ذهن شما باشد:

۱- می‌خواهم هر تغییری که برروی ساختار جداول، ایندکس‌ها، SP ها و... رخ می‌دهد، در جایی Log شود. در ضمن، در این Log گفته شود که کدام کلاینت این کار را انجام داده است.

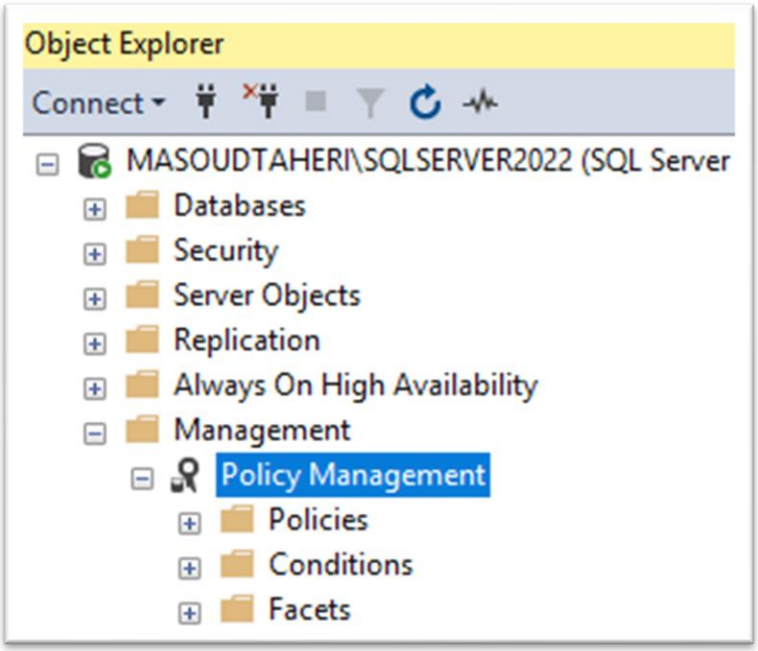
۲- در بانک اطلاعاتی خودم جدولی دارم که لیستی از IP هایی که مجاز به دسترسی هستند را مشخص کرده‌ام. می‌خواهم بدون داشتن فایروال کاری کنم که فقط این IP ها قابلیت دسترسی به بانک اطلاعاتی را داشته باشند.

در پاسخ به این سؤالات باید بگویم که انجام تمام این کارها با استفاده از DDL Trigger و Logon Trigger قابل انجام است.



بخش چهل و یکم: بررسی Policy Base Management

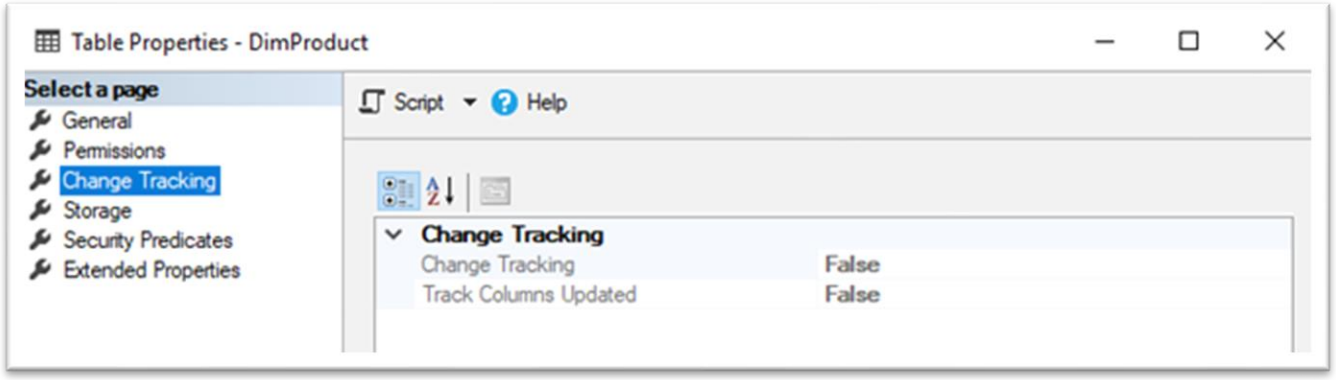
- PBM چیست؟
- بررسی مفهوم Facet
- بررسی نحوه نوشتن Expression و Condition برای Facet
- بررسی مفهوم Policy و اهداف آن در SQL Server
- بررسی نحوه ایجادکردن Policy
- بررسی Policy Category و نحوه ایجاد آن
- بررسی نحوه Evaluate کردن یک Policy



می‌خواهم در SQL Server یک چک لیست امنیتی ایجاد کنم و تمامی اشیاء موجود در بانک اطلاعاتی را با استفاده از آن مورد ارزیابی قرار دهم؛ به طوری که هرکدام از آن‌ها چنانچه با سیاست‌های تعریف‌شده مغایرت داشته باشد، به من گزارش داده شود. انجام این کار در SQL Server با استفاده از PBM امکان‌پذیر است

بخش چهل و دوم: استفاده از Change Tracking جهت پیاده‌سازی امنیت در SQL Server

- آشنایی با Change Tracking و مزایای آن
- بررسی نقش Change Tracking در امنیت بانک‌های اطلاعاتی
- بررسی معماری Change Tracking
- آشنایی با نحوه راه‌اندازی Change Tracking برروی جداول
- آشنایی با نحوه تأثیر دستورات DML برروی جداولی که دارای Change Tracking هستند
- آشنایی با نحوه استخراج نوع Action انجام‌شده برروی جداول دارای Change Tracking
- بررسی تنظیمات مربوط به Cleanup جداول Change Tracking

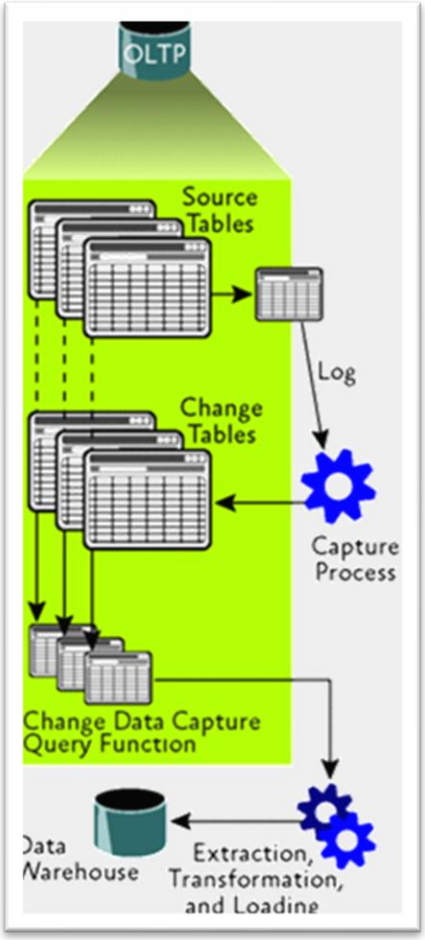


یکی از قابلیت‌های ساده در SQL Server در جهت کشف تغییرات مربوط به رکوردها، استفاده از ویژگی Change Tracking است. به وسیله این ویژگی می‌توان یک سناریو Auditing در سطح خیلی ساده برروی جداول پیاده‌سازی نمود.

بخش چهل و سوم: استفاده از Change Data Capture جهت پیاده‌سازی امنیت در SQL Server

- آشنایی با CDC و مزایای آن
- بررسی نقش جداول CDC در امنیت بانک‌های اطلاعاتی
- بررسی معماری CDC
- بررسی نحوه ایجاد جداول با پشتیبانی از CDC

- آشنایی با جداول سیستمی مربوط به CDC در SQL Server
- بررسی نحوه تأثیر دستورات DML برروی جداول CDC
- بررسی نحوه استخراج داده از جداول سیستمی CDC
- بررسی تنظیمات مربوط به Cleanup جداول CDC
- بررسی یک سناریو کاربردی برای استفاده از CDC جهت ذخیره سوابق تغییرات رکوردها

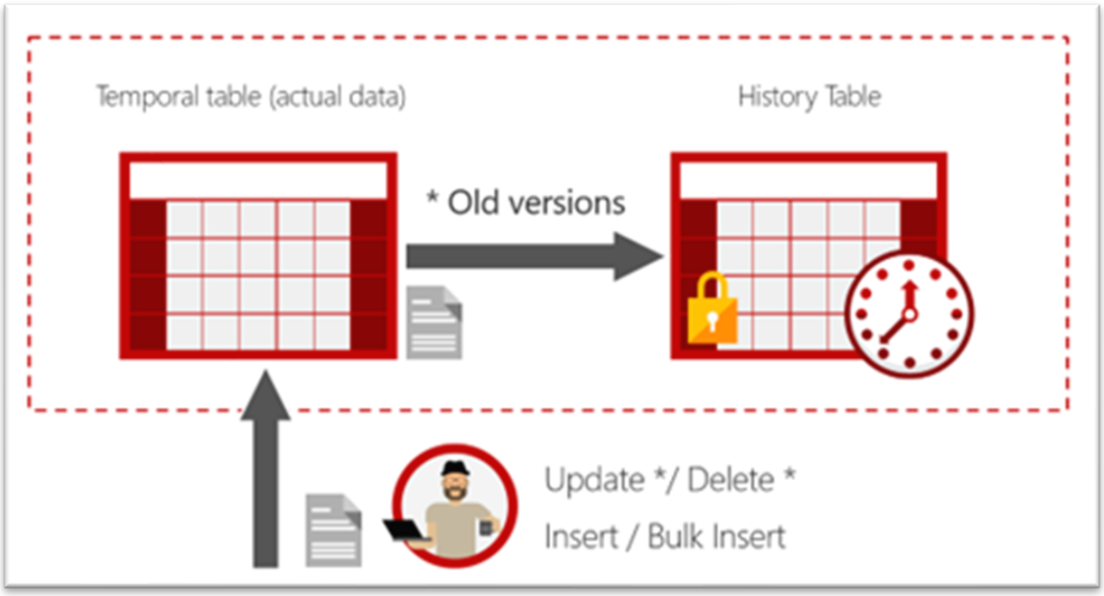


CDC یک ویژگی جالب در SQL Server در جهت ذخیره سوابق تغییرات رکوردها از روی Log File است. زمانی که این ویژگی را برروی جداول خود تنظیم نمایید، یک پروسه به‌صورت Asynchronously تغییرات رکوردهای جداول را استخراج و در جداولی سیستمی به‌همراه نوع Action ذخیره می‌نماید تا بعداً بتوان از آن استفاده نمود.

بخش چهل و چهارم: استفاده از Temporal Table جهت پیاده‌سازی امنیت در SQL Server

- آشنایی با Temporal Table و مزایای استفاده از آن
- بررسی نقش جداول Temporal در امنیت بانک‌های اطلاعاتی
- بررسی معماری Temporal Table
- بررسی نحوه ایجاد جداول با پشتیبانی از Temporal Table
- بررسی نحوه تأثیر دستورات DML برروی جداول Temporal
- بررسی نحوه نوشتن Temporal Query
- بررسی نحوه اعمال تنظیمات مناسب برروی جداول Temporal در جهت افزایش کارایی
- بررسی یک سناریو کاربردی برای استفاده از Temporal Table جهت ذخیره سوابق تغییرات رکوردها

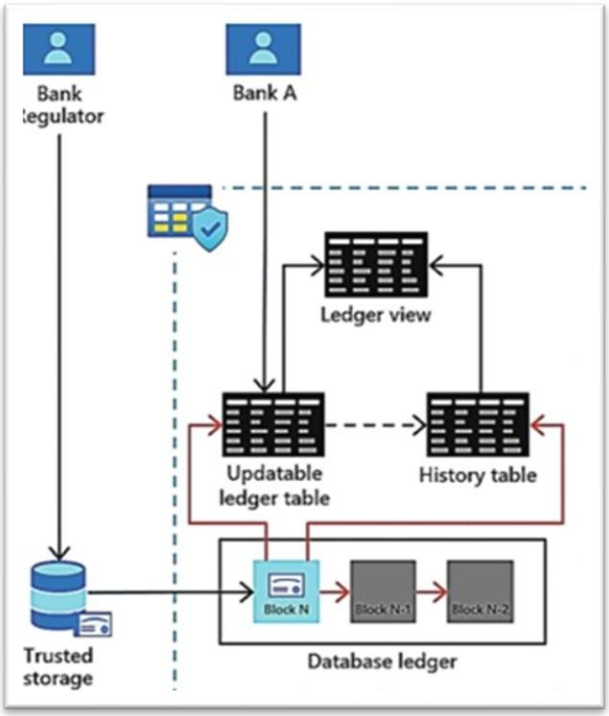
یکی از قابلیت‌هایی که در SQL Server برای ذخیره سوابق تغییرات رکوردها وجود دارد، استفاده از Temporal Table است. راه‌اندازی این ویژگی سریع و ساده است. برای مثال، این اواخر نیک آموز در یکی از پروژه‌های بزرگ خود، این ویژگی را برروی یک بانک اطلاعاتی بزرگ در یک سیستم کشوری راه‌اندازی کرد که بیش از ۸۰۰ میلیون رکورد تغییرات به وسیله این تکنولوژی جمع‌آوری شد.



بخش چهل و پنجم: استفاده از Database Ledger در SQL Server

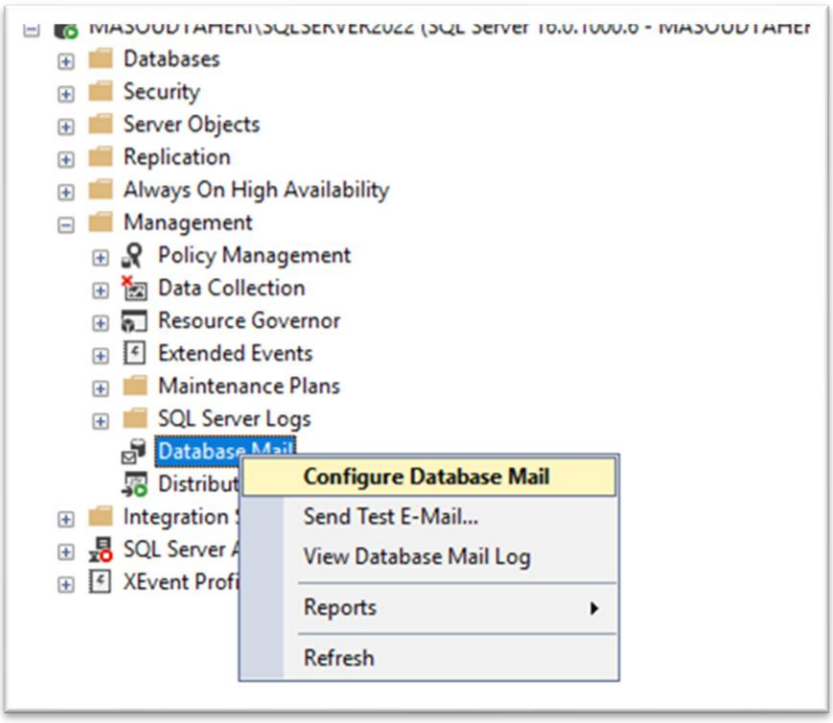
- بررسی Database Ledger
- بررسی Append only Ledger Tables
- بررسی Updatable Ledger Tables
- بررسی سناریوهای کاربردی برای کار با Database Ledger و Ledger Table ها
- بررسی محدودیت Ledger Table ها در SQL Server
- مقایسه Ledger Table ها با Temporal Table در SQL Server
- بررسی DMV های پرکاربرد در حوزه Database Ledger در SQL Server

Ledger Table ها نوع خاصی از جداول هستند که وظیفه آن‌ها محافظت از داده‌ها در برابر کاربران با دسترسی بالا است؛ به طوری که هرنوع عملیاتی برروی این نوع جداول انجام شود، سوابق تغییرات به‌صورت خودکار برروی جدول ذخیره‌شده و قابل ازبین رفتن نیست. این نوع جداول در قالب‌های مختلف در SQL Server ارائه شده و می‌توان سناریوهای مهم امنیتی را با آن جلو برد.



بخش چهل و ششم: استفاده از Database Mail در SQL Server

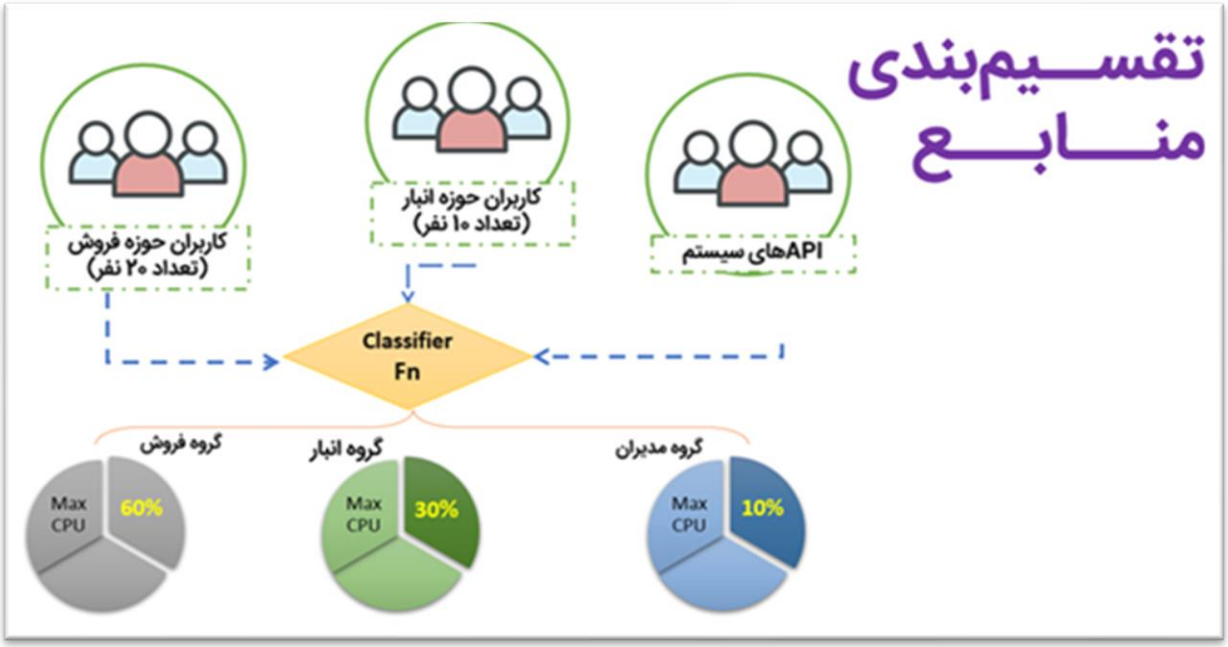
- معرفی ویژگی Database Mail
- بررسی معماری Database Mail
- نحوه پیکربندی Database Mail
- بررسی تنظیمات امنیتی برای دسترسی به Database Mail
- بررسی پروسیجر sp_send_dbmail
- بررسی سناریوهای امنیتی برای ارسال ایمیل در SQL Server



یکی از کارهای که در SQL Server برای اطلاع‌رسانی می‌توان انجام داد، راه‌اندازی Database Mail در جهت اطلاع‌رسانی رخدادهای مختلف است. برای مثال، با استفاده از این ویژگی می‌توان Error Log مربوط به SQL Server را بررسی و لیست Login Fail را استخراج و در قالب ایمیل اطلاع‌رسانی ارسال کرد.

بخش چهل و هفتم: بررسی Resource Governor

- Resource Governor چیست؟
- معرفی DOS Attack و روش جلوگیری آن در SQL Server
- بررسی نحوه استفاده از Resource Governor برای امن‌سازی SQL Server
- بررسی نحوه محدودکردن استفاده از Processor برای کاربران
- بررسی نحوه محدودکردن استفاده از Memory برای کاربران
- بررسی نحوه محدودکردن استفاده از IO برای کاربران
- بررسی تنظیمات مربوط به Query Governor در SQL Server
- بررسی DMV و DMF های مربوط به Resource Governor در SQL Server
- بررسی مفهوم Rate Limiter در API ها و تأثیر استفاده از آن در Database ها

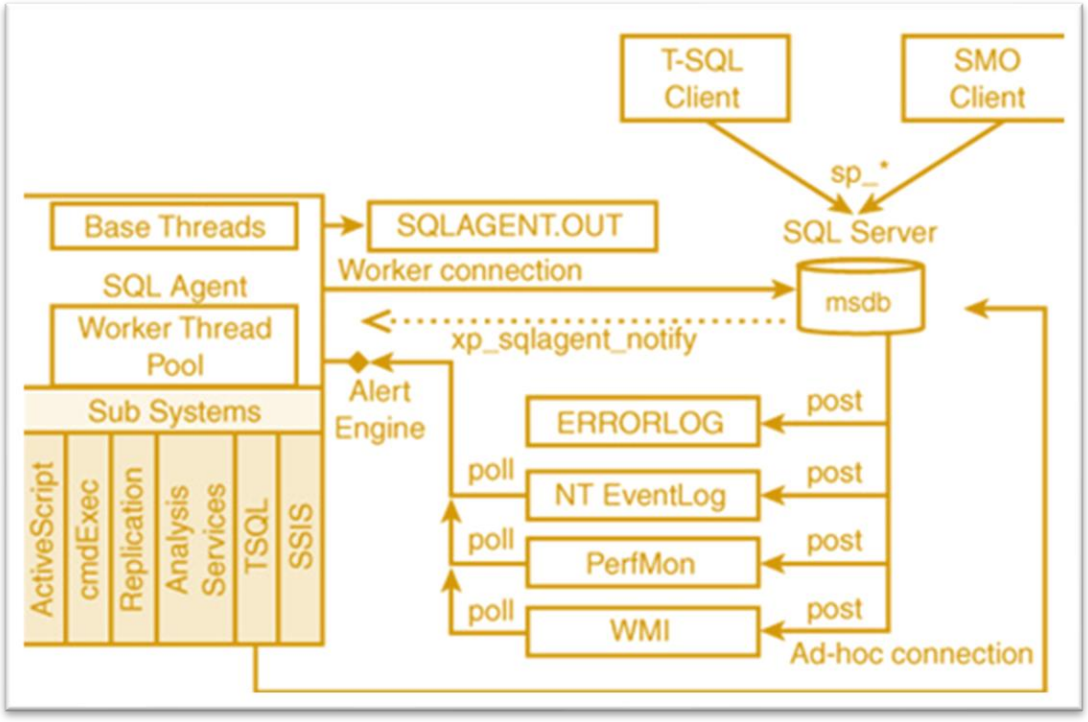


در یکی از سازمان‌های دولتی که مشغول به کار بودم، مشکلی وجود داشت. یک کوئری در طی چند ساعت، بیش از ۵ میلیون بار اجرا شده بود. با بررسی که انجام شد، متوجه شدم که کوئری موردنظر توسط یک وب‌سرویس که

برای App های بیرون از سازمان بود، نوشته شده است. این کوئری به ظاهر یک کوئری ساده بود که با حداقل IO دیتا را در دسترس کاربران قرار می‌داد؛ اما فراخوانی بیش از حد آن باعث مشغول بودن CPU شده. به‌طوری که خیلی‌ها فکر می‌کردند سرور، مورد Attack قرار گرفته است. برای اینکه بتوانیم کنترلی برروی دسترسی منابع به سرور داشته باشیم، با استفاده از Resource Governor این محدودیت را به‌وجود آوردیم.

بخش چهل و هشتم: بررسی سرویس Agent و نکات امنیتی مربوط به آن

- بررسی نحوه ایجاد JOB
- بررسی نحوه ایجاد Schedule برای Job ها
- بررسی تنظیمات امنیتی Job ها
- بررسی استفاده از Proxy ها در Job
- بررسی User برای اجرای JOB ها
- بررسی نحوه ایجاد Alert برای رخدادهای امنیتی با استفاده از Job
- بررسی بانک اطلاعاتی سیستمی MSDB و تنظیمات امنیتی مربوط به آن

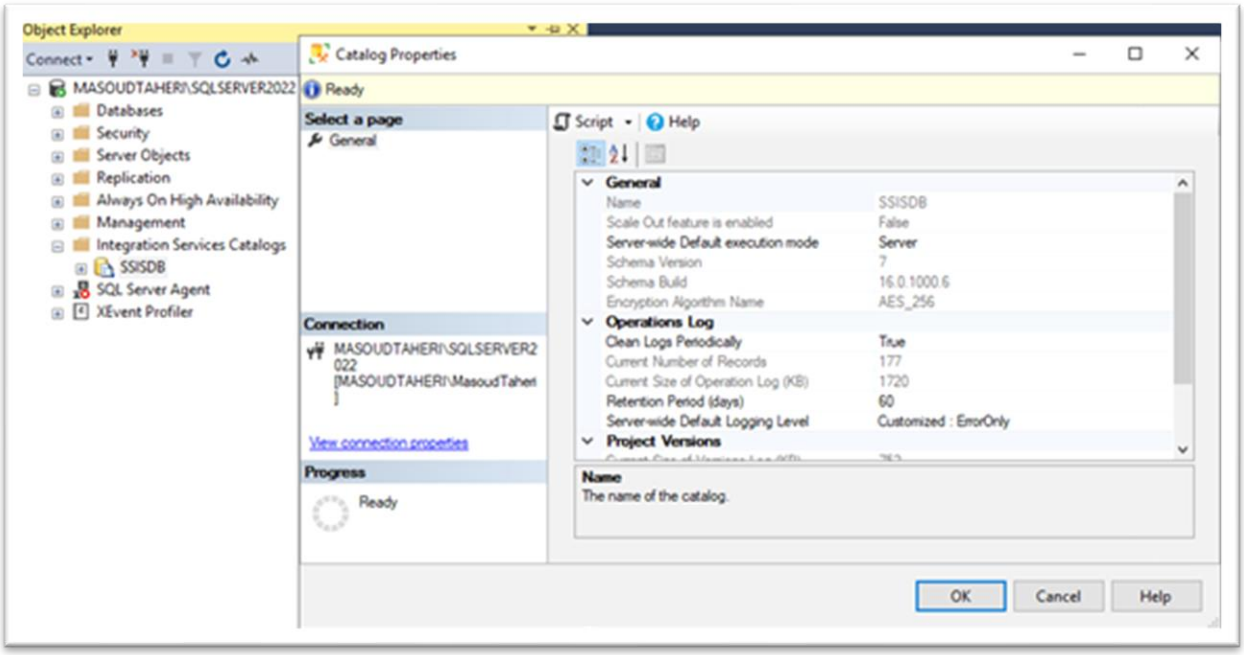


سرویس Agent یکی از مهم‌ترین سرویس‌های SQL Server بوده که وظیفه آن، اجرای فعالیت‌ها به‌صورت زمان‌بندی‌شده است. برای حفظ امنیت آن در SQL Server ویژگی‌های زیادی وجود دارد. بیشتر تنظیمات امنیتی مربوط به این سرویس در بانک اطلاعاتی msdb ذخیره می‌شود.

بخش چهل و نهم: بررسی سرویس SSIS و ارائه نکات امنیتی مربوط به آن

- معرفی مفهوم ETL
- بررسی سرویس SSIS
- بررسی Integration Catalog
- بررسی نحوه راه‌اندازی Integration Catalog
- بررسی بانک اطلاعاتی SSISDB و نقش‌های موجود در آن
- بررسی نکات امنیتی هنگام Deploy پکیج‌های SSIS

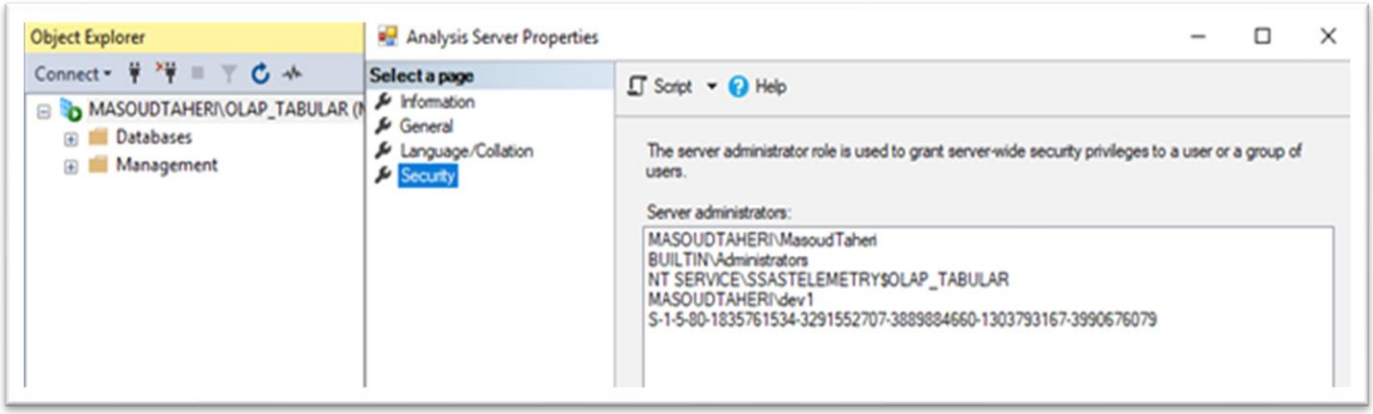
سرویس SSIS یکی از سرویس‌های کاربردی SQL Server در جهت پیاده‌سازی روال‌های ETL است. برای پیاده‌سازی روال‌های امنیتی در این سرویس باید تنظیمات اصولی مربوط به آن آشنا باشید. ما در طی این دوره، درخصوص تنظیمات امنیتی مربوط به این سرویس، نکات کاربردی را ارائه خواهیم داد.



بخش پنجاهم: بررسی سرویس SSAS و ارائه نکات مربوط به آن

- معرفی بانک‌های اطلاعاتی OLAP
- بررسی سرویس SSAS
- بررسی انواع مدل‌های OLAP
- بررسی سیستم امنیت OLAP
- بررسی تنظیمات امنیتی SSAS
- بررسی نحوه Deploy کردن یک بانک اطلاعاتی OLAP برروی سرور SSAS
- بررسی مفهموم Role و نحوه استفاده از آن در پروژه‌های OLAP

بانک‌های اطلاعاتی OLAP نوع خاصی از Database ها هستند که از آن‌ها برای تحلیل استفاده می‌شود. معماری امنیت این بانک‌ها با معماری بانک‌های اطلاعاتی عملیاتی متفاوت است. ما در طی این دوره، شما را با مباحث امنیتی مربوط به این نوع بانک‌های اطلاعاتی آشنا خواهیم کرد.



بخش پنجاه و یکم: معرفی ابزارهای کاربردی در حوزه امنیت SQL Server

- ارائه اسکریپت‌های پرکاربرد در حوزه امنیت متناسب با درس هر حوزه
- معرفی ابزار Wireshark برای مانیتورکردن ترافیک SQL Server
- آموزش ابزار تخصصی برای Block کردن حملات Brute-Force در SQL Server
- معرفی ابزار SQL Password Recovery
- معرفی ابزار Reflector و نحوه استفاده از آن در SQL Server
- معرفی ابزار SQL Decryptor و نحوه کار با آن در SQL Server

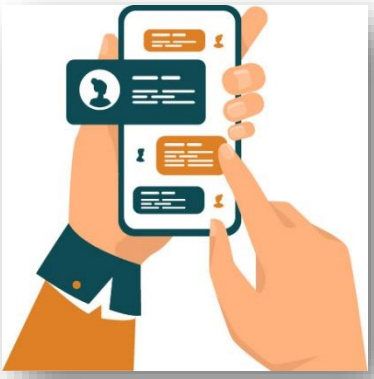
در طی دوره با توجه به سناریوهای آموزشی ارائه‌شده، تعدادی ابزار مفید انتخاب شده که کار کردن با هرکدام از آن‌ها را در طی جلسات مختلف خواهیم داشت.

مدرس: مسعود طاهری

نحوه مشاهده دوره چگونه است؟

این دوره آموزشی را می‌توانید در یک پلیر اختصاصی مشاهده فرمایید. به‌راحتی می‌توانید این نرم‌افزار را مناسب با سیستم عامل خود (ویندوز، مک، اندروید، لینوکس و یا وب) دانلود نصب کرده و پس از کپی کلید لایسنس داخل نرم‌افزار، محصول خریداری شده را تماشا کنید.

صدور فاکتور رسمی چگونه است؟



در صورت تمایل به دریافت فاکتور رسمی، پیش از خرید خود با واحد فروش مجموعه (۱۷ ۰۰ ۹۱ ۰۷ – ۰۲۱) تماس حاصل نمایید.**شایان ذکر است، امکان صدور فاکتور رسمی پس از خرید آنلاین از سایت مجموعه به هیچ عنوان وجود نخواهد داشت.**

آدرس: تهران، یوسف آباد، میدان فرهنگ، خیابان ۳۳، پلاک ۲۹، زنگ ۲، دفتر نیک آموز

شماره تماس: ۱۷ ۰۰ ۹۱ ۰۷ – ۰۲۱ | **موبایل فروش:** ۲۰۶ ۴۰۰۶ ۰۹۱۰