



بررسی و رفع خطای "Cannot generate SSPI context" در محیط‌های (Domain) و SQL Server

نویسنده: احمد کارزنوی

سمت: کارشناس دیتابیس

نوع مقاله: پژوهشی

نوشته شده در تاریخ: ۱۴۰۵/۰۵/۰۱

چکیده:

خطای Cannot generate SSPI context با پیام همراه The target principal name is incorrect یکی از چالش‌های رایج در محیط‌های مبتنی بر دامنه (Domain) به ویژه هنگام اتصال به SQL Server از طریق احراز هویت ویندوز (Windows Authentication) است. این خطا عمدتاً ناشی از پیکربندی ناصحیح نام‌های اصلی سرویس (Service Principal Names - SPN) در سرویس‌های دایرکتوری اکتیو (Active Directory) و در نتیجه شکست فرآیند احراز هویت کربروس (Kerberos) می‌باشد. در این مقاله، ابتدا به تشریح مفهوم SSPI Context و نقش آن در احراز هویت پرداخته، سپس علل بروز خطا را بررسی کرده و در نهایت روش‌های گام‌به‌گام رفع مشکل، شامل اصلاح SPN از طریق ابزارهای گرافیکی Active Directory و خط فرمان، ارائه می‌شود. همچنین سایر عوامل مؤثر نظیر مشکلات DNS، هم‌زمان‌سازی زمان و استفاده از نام‌های مستعار (Alias) مورد بررسی قرار گرفته و بهترین شیوه‌های پیاده‌سازی در محیط‌های تولیدی پیشنهاد می‌گردد.

مقدمه

در بسیاری از سازمان‌ها و مؤسسات آموزشی، استفاده از SQL Server با احراز هویت ویندوز و در بستر دامنه (Active Directory) رایج است. این روش احراز هویت، امنیت بالا و مدیریت متمرکز کاربران را فراهم می‌آورد. با این حال، پیکربندی نادرست برخی از مؤلفه‌های زیرساخت، به ویژه در حوزه احراز هویت کربروس، می‌تواند منجر به بروز خطاهایی در فرآیند اتصال گردد. خطای Cannot generate SSPI context از جمله رایج‌ترین این خطاهاست که اغلب با پیام The target principal name is incorrect همراه است. درک صحیح از نحوه عملکرد کربروس و نقش SPN، کلید اصلی عیب‌یابی و رفع این مشکل محسوب می‌شود.



مفهوم SSPI Context

SSPI (Security Support Provider Interface) یک رابط برنامه‌نویسی در سیستم عامل ویندوز است که امکان استفاده از پروتکل‌های مختلف احراز هویت از جمله کربروس و NTLM را فراهم می‌سازد. هنگامی که یک برنامه کاربردی (مانند SQL Server Management Studio) قصد اتصال به SQL Server را با استفاده از احراز هویت ویندوز دارد، فرآیند زیر رخ می‌دهد:

- ۱- کلاینت (برنامه کاربر) درخواست بلیت (Ticket) خود را به کنترل‌کننده دامنه (Domain Controller) ارسال می‌کند.
 - ۲- کنترل‌کننده دامنه بر اساس SPN ثبت‌شده برای سرویس مورد نظر در اینجا (SQL Server)، اعتبار درخواست را بررسی می‌کند.
 - ۳- در صورت صحت SPN، کنترل‌کننده دامنه یک بلیت کربروس صادر کرده و به کلاینت تحویل می‌دهد.
 - ۴- کلاینت این بلیت را به SQL Server ارائه می‌دهد و SQL Server پس از تأیید آن توسط کنترل‌کننده دامنه، احراز هویت را می‌پذیرد.
- اگر هر یک از این مراحل با خطا مواجه شود، فرآیند تولید SSPI Context شکست خورده و خطای مورد نظر ظاهر می‌شود. در اغلب موارد، دلیل اصلی این شکست، ناهماهنگی بین حساب کاربری که سرویس SQL Server تحت آن اجرا می‌شود و SPN ثبت شده در Active Directory است.

علت اصلی بروز خطا (سناریوی رایج)

در بسیاری از سازمان‌ها، SQL Server با یک حساب کاربری دامنه (Domain Account) به عنوان حساب سرویس (Service Account) اجرا می‌شود، برای مثال DOMAIN\sqlsvc. به دلایل مختلف از جمله استفاده از ابزارهای نصب خودکار یا اقدامات اشتباه مدیران، ممکن است SPN مربوط به سرویس SQL Server بر روی شیء رایانه (Computer Object) سرور ثبت شود، در حالی که باید بر روی خود حساب سرویس (User Object) ثبت گردد. این تناقض باعث می‌شود که کنترل‌کننده دامنه نتواند سرویس را به درستی شناسایی کرده و احراز هویت کربروس با شکست مواجه شود.

نمونه‌ای از پیکربندی اشتباه:

- SQL Server بر روی سروری با نام SQLSERVER01 اجرا می‌شود.
- حساب سرویس DOMAIN\sqlsvc است.
- SPN مانند MSSQLSvc/SQLSERVER01:1433 به اشتباه بر روی شیء رایانه (Computer Object) SQLSERVER01 ثبت شده است.

این وضعیت، ریشه اصلی خطای مذکور در بسیاری از موارد است.



روش جامع رفع مشکل

رفع این خطا شامل دو بخش کلی است: ابتدا باید SPN های نادرست را از شیء رایانه حذف کرده و سپس SPN های صحیح را بر روی حساب سرویس ثبت کنیم. در ادامه، هر دو بخش به تفصیل شرح داده شده است.

اصلاح SPN از طریق Active Directory

این روش در محیط های سازمانی و آموزشی که دسترسی به رابط کاربری Active Directory وجود دارد، بسیار کاربردی و رایج است.

مرحله ۱: ورود به Active Directory Users and Computers

بر روی یکی از کنترل کننده های دامنه، ابزار Active Directory Users and Computers (ADUC) را اجرا کنید.

مرحله ۲: فعال سازی نمایش ویژگی های پیشرفته

از نوار منوی بالای ابزار، گزینه View را انتخاب کرده و سپس گزینه Advanced Features را فعال کنید. این کار امکان مشاهده و ویرایش ویژگی های پیشرفته اشیاء را فراهم می سازد.

مرحله ۳: یافتن شیء رایانه مربوط به سرور SQL Server

در درخت سمت چپ، به گره Computers یا محل قرارگیری سرور مورد نظر بروید و شیء رایانه (Computer Object) مربوط به سرور SQL Server را پیدا کنید.

مرحله ۴: دسترسی به ویرایشگر ویژگی ها (Attribute Editor)

بر روی شیء رایانه راست کلیک کرده و گزینه Properties را انتخاب کنید. در پنجره باز شده، به برگه Attribute Editor بروید. (توجه: این برگه تنها در صورت فعال بودن Advanced Features قابل مشاهده است).

مرحله ۵: یافتن ویژگی service Principal Name

در لیست ویژگی ها، ویژگی با نام service Principal Name را پیدا کنید. این ویژگی حاوی لیست تمام SPN های ثبت شده بر روی آن شیء است.

مرحله ۶: حذف SPN های اشتباه

در لیست مقادیر ویژگی servicePrincipalName، به دنبال مقادیری مشابه نمونه های زیر بگردید:

- MSSQLSvc/ServerName:1433

- MSSQLSvc/ServerName.domain.local:1433



اگر سرویس SQL Server بر روی یک حساب کاربری دامنه (غیر از حساب رایانه) اجرا می شود، این SPN ها نباید بر روی شیء رایانه وجود داشته باشند. آنها را انتخاب کرده و با کلیک بر روی دکمه Remove حذف کنید.

مرحله ۷: انتظار برای همسازي (Replication)

پس از اعمال تغییرات، چند دقیقه صبر کنید تا تغییرات بین کنترل کننده های دامنه همسازي (Replicate) شوند.

مرحله ۸: پاکسازی کش کربروس در سمت کلاینت

برای اطمینان از اعمال تغییرات، بر روی کلاینت (سیستمی که اتصال از آن برقرار می شود) دستور زیر را در خط فرمان با دسترسی مدیر اجرا کنید تا کش بلیت های کربروس پاک شود:

cmd

klist purge

ثبت صحیح SPN بر روی حساب سرویس

پس از حذف SPN های اشتباه، باید SPN های صحیح را بر روی حساب کاربری سرویس (Service Account) ثبت کنیم. برای این کار از ابزار خط فرمان setspn.exe استفاده می شود.

ثبت SPN اصلی و SPN با نام کامل دامنه: (FQDN)

```
setspn -A MSSQLSvc/ServerName:1433 DOMAIN\sqlsvc
```

```
setspn -A MSSQLSvc/ServerName.domain.local:1433 DOMAIN\sqlsvc
```

در دستورات فوق:

- ServerName نام NetBIOS سرور SQL Server است.
- ServerName.domain.local نام کامل دامنه (Fully Qualified Domain Name) سرور است.
- 1433 شماره پورت پیش فرض SQL Server است. در صورت استفاده از پورت غیر پیش فرض، شماره پورت مربوطه باید وارد شود.
- DOMAIN\smlsvc نام حساب کاربری سرویس در قالب دامنه نام کاربری است.

پس از اجرای این دستورات، SPN ها بر روی حساب سرویس ثبت خواهند شد. می توانید با دستور زیر صحت ثبت را بررسی کنید:

```
setspn -L DOMAIN\smlsvc
```



بررسی سایر عوامل مؤثر در بروز خطا

اگر چه مشکل اصلی در اغلب موارد به SPN برمی گردد، اما عوامل دیگری نیز می توانند باعث بروز خطای مشابه شوند. در ادامه به مهم ترین آنها اشاره می شود.

وجود SPN تکراری (Duplicate SPN)

اگر یک SPN به طور همزمان بر روی دو شیء مختلف در Active Directory مثلاً هم بر روی Computer Object و هم بر روی User Object ثبت شده باشد، کنترل کننده دامنه در تشخیص سرویس دچار ابهام شده و احراز هویت با شکست مواجه می شود. برای شناسایی SPN های تکراری از دستور زیر استفاده کنید:

setspn -X

این دستور تمام SPN های تکراری را در سراسر دامنه لیست می کند. در صورت مشاهده تکراری، باید یکی از آنها را حذف کنید.

مشکلات مربوط به سامانه نام دومین (DNS)

اگر نام سرور به درستی توسط کلاینت به آدرس IP تبدیل نشود، فرآیند احراز هویت کربروس با مشکل مواجه می شود. برای بررسی صحت عملکرد DNS از دستورات زیر استفاده کنید:

nslookup ServerName

ping ServerName

اطمینان حاصل کنید که نام سرور چه NetBIOS و چه FQDN به درستی به آدرس IP صحیح سرور اشاره دارد.

استفاده از آدرس IP به جای نام سرور

یکی از اشتباهات رایج، استفاده از آدرس IP به جای نام سرور در رشته اتصال (Connection String) است. احراز هویت کربروس به نام سرویس (Service Name) وابسته است و استفاده از IP باعث می شود که کلاینت نتواند SPN صحیح را پیدا کند. همیشه از نام کامل سرور ترجیحاً (FQDN) در رشته اتصال استفاده کنید.

مثال نادرست:

10.10.10.5

مثال صحیح:

SQLSERVER01.domain.local



مشکل همزمانی زمان (Time Synchronization)

پروتکل کربروس به همزمانی زمان بین کلاینت، سرور و کنترل کننده دامنه حساس است. اختلاف زمانی بیش از حد مجاز (معمولاً ۵ دقیقه) می تواند باعث رد شدن بلیت ها شود. برای بررسی وضعیت همزمانی زمان از دستور زیر استفاده کنید:

```
w32tm /query /status
```

در محیط های دامنه، توصیه می شود که تمام سرورها و کلاینت ها زمان خود را با کنترل کننده دامنه همزمان کنند.

استفاده از نام های مستعار (SQL Alias)

اگر از SQL Server Alias برای اتصال به پایگاه داده استفاده می کنید، لازم است که SPN مربوط به آن نام مستعار نیز بر روی حساب سرویس ثبت شود. به عنوان مثال، اگر نام مستعار SQLAlias تعریف شده است، باید SPN زیر را نیز اضافه کنید:

```
setspn -A MSSQLSvc/SQLAlias:1433 DOMAIN\sqsvc
```

تأیید نهایی و تست اتصال

پس از انجام اصلاحات، برای اطمینان از صحت پیکربندی و رفع خطا، مراحل زیر را انجام دهید.

بررسی بلیت های کربروس در سمت کلاینت

دستور زیر را در خط فرمان کلاینت اجرا کنید:

```
klist
```

در خروجی، باید بلیت هایی با نام سرویس MSSQLSvc مربوط به سرور SQL Server مشاهده کنید. وجود این بلیت ها نشان دهنده موفقیت آمیز بودن فرآیند احراز هویت کربروس است.

بررسی روش احراز هویت در SQL Server

با اتصال به SQL Server مثلاً با استفاده از (SQL Server Management Studio)، کوئری زیر را اجرا کنید:

```
SELECT auth_scheme
```

```
FROM sys.dm_exec_connections
```

```
WHERE session_id = @@SPID;
```

خروجی این کوئری باید KERBEROS باشد. اگر خروجی NTLM باشد، نشان می دهد که احراز هویت از طریق کربروس انجام نشده و ممکن است هنوز مشکلی وجود داشته باشد.



بهترین شیوه‌های پیاده‌سازی در محیط تولید (Production Best Practices)

برای جلوگیری از بروز مجدد این خطا و اطمینان از عملکرد صحیح احراز هویت در محیط‌های تولیدی، رعایت نکات زیر توصیه می‌شود:

- SQL Server همواره با یک حساب کاربری دامنه (Domain Service Account) مجزا و با حداقل دسترسی‌های لازم اجرا شود.
 - SPNها تنها بر روی حساب سرویس (User Object) ثبت شوند و هرگز بر روی شیء رایانه (Computer Object) قرار نگیرند.
 - از اتصال به SQL Server از طریق آدرس IP خودداری شده و همواره از نام کامل دامنه (FQDN) استفاده شود.
 - سلامت سرویس‌های DNS در شبکه به طور مستمر پایش شود.
 - همزمانی زمان (Time Synchronization) تمام گره‌ها با کنترل‌کننده دامنه به دقت تنظیم گردد.
 - در صورت تغییر حساب سرویس SQL Server، بلافاصله SPNهای مربوطه بررسی و به‌روزرسانی شوند.
- برای محیط‌های بزرگ، استفاده از اسکریپت‌های خودکار برای ثبت و مدیریت SPNها توصیه می‌شود.

نتیجه گیری

خطای Cannot generate SSPI context با پیام The target principal name is incorrect عمدتاً به دلیل پیکربندی نادرست SPN در Active Directory رخ می‌دهد. با درک صحیح از نقش SPN در احراز هویت کربروس و انجام اصلاحات مورد نیاز - شامل حذف SPNهای اشتباه از شیء رایانه و ثبت صحیح آنها بر روی حساب سرویس - می‌توان این خطا را در بیش از ۹۰ درصد موارد برطرف کرد. همچنین توجه به عواملی نظیر یکتایی SPNها، صحت رکوردهای DNS، همزمانی زمان و استفاده از نام‌های صحیح در رشته اتصال، از بروز مجدد مشکل جلوگیری می‌کند. رعایت بهترین شیوه‌های ارائه‌شده در این مقاله، به مدیران و کارشناسان فناوری اطلاعات کمک می‌کند تا زیرساخت امن و پایداری برای سرویس‌های SQL Server در محیط‌های دامنه فراهم آورند.

منابع پیشنهادی برای مطالعه بیشتر

- مستندات رسمی مایکروسافت در مورد پیکربندی SPN برای SQL Server (Microsoft Docs)
- راهنمای عیب‌یابی احراز هویت کربروس در ویندوز سرور
- مقاله‌های مرتبط با مدیریت Active Directory و DNS در محیط‌های سازمانی