راهنمای نصب دستی Inogen برای مشتری

در نمونه‌های زیر، سرور SQL برابر `SQL-SERVER-01`، دیتابیس جدید برابر `Inogen_CompanyA`، دامنهٔ فرانت برابر `app.example.com` و دامنهٔ API برابر `api.example.com` است. این مقدارها را با مقدار واقعی خود جایگزین کنید. فرمان‌ها را از ریشهٔ بستهٔ استخراج‌شده اجرا کنید.

۱. سرور و فایل‌ها را آماده کنید

1. روی IIS ،Windows Server با قابلیت‌های Static Content و Default Document، افزونه URL Rewrite و .NET Hosting Bundle سازگار با API را نصب کنید.
2. برای دامنه‌های فرانت و API رکورد DNS تنظیم کنید. گواهی HTTPS معتبر هر دامنه را روی سرور IIS نصب کنید؛ گواهی CDN به‌تنهایی گواهی IIS نیست.
3. ZIP را در پوشه‌ای مانند `C:\Inogen` استخراج کنید. پوشه‌های `frontend` و `backend` را کنار هم نگه دارید؛ فرمان‌های نصب را از ریشهٔ بسته اجرا کنید.

۲. دیتابیس و حساب‌ها را آماده کنید

1. در SQL Server یک دیتابیس خالی با نام واقعی استقرار، مانند `Inogen_CompanyA`، ایجاد کنید.
2. در SSMS به همان نمونهٔ SQL Server که دیتابیس را در آن ساخته‌اید، با حساب مدیر وصل شوید. از بخش `Security > Logins` حساب SQL به نام `inogen_migrator` را بسازید یا وجود آن را بررسی کنید. در یک پنجرهٔ Query همان اتصال، نام دیتابیس را در فرمان زیر جایگزین و آن را اجرا کنید تا کاربر دیتابیس ساخته شود و مجوز اجرای migration بگیرد:

```
USE [Inogen_CompanyA]; IF USER_ID(N'inogen_migrator') IS NULL CREATE USER [inogen_migrator] FOR LOGIN [inogen_migrator]; IF IS_ROLEMEMBER(N'db_owner', N'inogen_migrator') <> 1 ALTER ROLE [db_owner] ADD MEMBER [inogen_migrator];
```

حساب جداگانهٔ `inogen_runtime` را برای API بسازید؛ پس از اجرای migration به آن مجوزهای `SELECT`، `INSERT`، `UPDATE` و `DELETE` روی schema `inogen` بدهید. به حساب runtime مجوز تغییر ساختار ندهید. 3. پیش از اجرای migration، یک اتصال جدید در SSMS با SQL Authentication و حساب `inogen_migrator` به همان نمونهٔ SQL باز کنید. فرمان زیر را با نام دیتابیس واقعی اجرا کنید. مقدارهای `IsDbOwner` و `CanCreateTable` باید هر دو `1` باشند. اگر اتصال برقرار نشد یا یکی از مقدارها `1` نبود، نگاشت کاربر، نقش و نام نمونهٔ SQL را با مدیر سرور اصلاح کنید و سپس این بررسی را تکرار کنید:

```
USE [Inogen_CompanyA]; SELECT @@SERVERNAME AS SqlServer, DB_NAME() AS DatabaseName, ORIGINAL_LOGIN() AS LoginName, USER_NAME() AS DatabaseUser, IS_MEMBER(N'db_owner') AS IsDbOwner, HAS_PERMS_BY_NAME(DB_NAME(), N'DATABASE', N'CREATE TABLE') AS CanCreateTable;
```

1. گواهی TLS سرور SQL را روی سرور برنامه مورد اعتماد قرار دهید. رشته‌های اتصال را با `Encrypt=True;TrustServerCertificate=False` تنظیم کنید.

۳. تنظیمات را ثبت و migration را اجرا کنید

1. در `backend\appsettings.Production.json`، مقدارهای نمونهٔ `AllowedServers`، `AllowedDatabases` و `FrontendOrigins` را با سرور SQL، دیتابیس مقصد و نشانی فرانت واقعی جایگزین کنید. مقدار `ApplyMigrationsOnStartup` را `false` نگه دارید. مقدار `TargetDatabase` فقط نمونه است؛ رمز `CHANGE_ME` را در فایل به رمز واقعی تبدیل نکنید. رشتهٔ اتصال واقعی را در گام IIS، برای App Pool API ثبت کنید.

2. در `frontend\config\runtime-config.js` نشانی API را ثبت کنید:

```
window.INOGEN_CONFIG = { apiBaseUrl: "https://api.example.com/api/v1" };
```

فایل را در پوشهٔ `frontend` **نسخهٔ نصب‌شده روی سرور** نیز بررسی کنید؛ مقدار `/api/v1` فقط زمانی درست است که API و فرانت روی یک دامنه و از همان مسیر منتشر شده باشند. برای دو دامنهٔ جدا، نشانی کامل HTTPS دامنهٔ API را مانند نمونهٔ بالا بگذارید. در `backend\appsettings.Production.json` نیز نشانی واقعی دامنهٔ فرانت را در `FrontendOrigins` ثبت کنید.

1. در PowerShell، پس از اصلاح `AllowedServers` و `AllowedDatabases` در فایل تنظیمات، فرمان زیر را از ریشهٔ بسته اجرا کنید. نام حساب SQL را جایگزین کنید؛ اسکریپت نام سرور و دیتابیس را از همان فایل می‌خواند و رمز را جداگانه درخواست می‌کند:

```
.\migrate-target.ps1 -SqlUser 'inogen_migrator'
```

فقط پس از دیدن `Target migrations applied.` ادامه دهید و همین پنجرهٔ PowerShell را برای ساخت حساب مدیر باز نگه دارید. migration ساختار دیتابیس را ایجاد می‌کند و دادهٔ قدیمی را منتقل نمی‌کند. اگر گواهی SQL فقط در محیط تست مورد اعتماد نیست، می‌توانید موقتاً `-TrustServerCertificate` را به انتهای همین فرمان اضافه کنید.

اگر خطای `SQL error 262: CREATE TABLE permission denied` دیدید، migration را متوقف کنید؛ گام ۲ و ۳ بخش «دیتابیس و حساب‌ها» را روی همان نمونهٔ SQL و همان دیتابیس تکرار کنید. پیام `Target guard passed` فقط نام مقصد را بررسی می‌کند و تأیید مجوز SQL نیست. پس از اینکه هر دو مقدار بررسی مجوز `1` شدند، فرمان migration را دوباره اجرا کنید. اگر خطای گواهی نامعتبر دیدید، گواهی SQL را روی سرور برنامه مورد اعتماد قرار دهید؛ گزینهٔ `TrustServerCertificate` فقط برای تست داخلی است.

1. پس از migration، در SSMS مجوز حساب runtime را روی دیتابیس مقصد ثبت کنید:

```
USE [Inogen_CompanyA]; IF USER_ID(N'inogen_runtime') IS NULL CREATE USER [inogen_runtime] FOR LOGIN [inogen_runtime]; GRANT SELECT, INSERT, UPDATE, DELETE ON SCHEMA::[inogen] TO [inogen_runtime];
```

۴. سایت‌های IIS را دستی ایجاد کنید

1. در IIS Manager دو Application Pool به نام `Inogen-Frontend` و `Inogen-Api` بسازید و `.NET CLR Version` را برای هر دو روی `No Managed Code` بگذارید.

2. سایت فرانت را به مسیر فیزیکی `C:\Inogen\frontend` و Pool اول وصل کنید. سایت API را به `C:\Inogen\backend` و Pool دوم وصل کنید. اگر مسیر استخراج متفاوت است، همان مسیر واقعی را وارد کنید.
3. برای هر سایت binding از نوع `https` روی پورت `443` و Host name همان دامنه با SNI بسازید و گواهی همان دامنه را انتخاب کنید. اگر از ابر آروان استفاده می‌کنید، HTTPS از آروان تا سرور مبدأ را نیز تنظیم کنید.
4. به `IIS AppPool\Inogen-Api` روی `backend\data` و زیرپوشه‌های آن مجوز Modify بدهید.
5. رشتهٔ اتصال حساب runtime را با نام `ConnectionStrings__TargetDatabase` در **متغیرهای محیطی App Pool API** ثبت کنید. نمونهٔ مقدار در `appsettings.Production.json` آمده است؛ رمز واقعی را در آن فایل ننویسید. پس از ساخت Pool، در PowerShell مدیر فرمان زیر را اجرا کنید. اسکریپت نام سرور و دیتابیس را از فایل تنظیمات می‌خواند و رمز را جداگانه می‌پرسد:

```
.\set-iis-runtime-connection.ps1 -SqlUser 'inogen_runtime' -AppPoolName 'Inogen-Api'
```

این مقدار در تنظیمات IIS ذخیره می‌شود؛ دسترسی مدیران سرور به آن را محدود کنید. اگر نام Pool را تغییر داده‌اید، مقدار `-AppPoolName` را عوض کنید. در محیط تست، اگر گواهی SQL هنوز مورد اعتماد نیست، گزینهٔ `TrustServerCertificate` را فقط موقتاً به فرمان اضافه کنید.

1. از خود سرور، `https://api.example.com/health` و سپس `https://api.example.com/api/v1/deployment/profile` را باز کنید. پاسخ اول باید کد `200` و پاسخ دوم باید یک شیء JSON شامل `company`، `branding` و `activation` باشد. سپس نشانی فرانت را باز کنید. اگر فرانت پیام «تنظیمات استقرار در دسترس نیست» نشان داد، ابتدا `frontend\config\runtime-config.js` را بررسی کنید و سپس در ابزار Developer Tools مرورگر، وضعیت درخواست `/api/v1/deployment/profile` را ببینید. اگر درخواست به دامنهٔ اشتباه می‌رود، نشانی API را در همان فایل اصلاح و صفحه را با بارگذاری کامل دوباره باز کنید؛ اگر درخواست از دامنهٔ درست خطای شبکه یا CORS دارد، HTTPS دامنهٔ API و مقدار `FrontendOrigins` را بررسی کنید.

۵. سامانه را فعال و مدیر را ایجاد کنید

1. نشانی فرانت را مانند `https://app.example.com/admin` باز کنید. اگر صفحهٔ فعال‌سازی نمایش داده شد، شناسهٔ ۶۴ کاراکتری سرور را کپی و برای صادرکنندهٔ کد ارسال کنید. کد دریافتی را در همان صفحه ثبت کنید.
2. در همان نشست PowerShell گام ۳، حساب مدیر را روی همان دیتابیس بسازید. اگر PowerShell را بسته‌اید، ابتدا اتصال را در نشست جدید با فرمان زیر دوباره آماده کنید؛ `-ConfigureOnly` migration را تکرار نمی‌کند:

```
.\migrate-target.ps1 -SqlUser 'inogen_migrator' -ConfigureOnly
```

اگر فقط در محیط تست گواهی SQL هنوز مورد اعتماد نیست، به همین فرمان `-TrustServerCertificate` را هم اضافه کنید. سپس در همان پنجره حساب مدیر را بسازید:

```
.\initialize-admin.ps1 -DisplayName 'مدیر سامانه'
```

رمز مدیر باید حداقل ۱۲ نویسه، حرف بزرگ، حرف کوچک، رقم و نویسهٔ ویژه داشته باشد. نام کاربری خروجی را ثبت کنید و رمز را جداگانه و امن تحویل دهید. حساب مدیر با رمز پیش‌فرض وجود ندارد.

پس از فعال‌سازی و ورود مدیر، صفحهٔ تنظیمات استقرار را مستقیم با نشانی مانند `https://app.example.com/admin/deployment-settings` باز کنید. این صفحه در منوی پنل نمایش داده نمی‌شود. در بخش `واحدهای داشبورد` نام واحدها و چیدمان را ثبت کنید و دکمهٔ `ذخیره تنظیمات` را بزنید. صفحهٔ ورود کد فعال‌سازی فقط کد را دریافت می‌کند؛ تنظیمات واحدها در صفحهٔ جداگانه انجام می‌شود.

اگر ساخت مدیر ناموفق بود، مرحلهٔ اعلام‌شده در خطای ابزار را بخوانید. برای خطای `Identity validation failed`، کد خطای سیاست رمز یا نام کاربری را اصلاح و فرمان را دوباره اجرا کنید. اگر نشست PowerShell عوض شده است، ابتدا فرمان `migrate-target.ps1` را با `-ConfigureOnly` در همان نشست اجرا کنید و سپس ساخت مدیر را تکرار کنید. اگر خطا در مرحلهٔ `create roles` یا `assign administrator role` رخ داد، مجوز حساب migration را روی دیتابیس مقصد بررسی کنید؛ حساب API را برای این فرمان به کار نبرید.

۶. نصب را بررسی کنید

1. نشانی پنل مدیر را با دامنهٔ واقعی فرانت، مانند `https://app.example.com/admin`، باز کنید و با حساب مدیری که در گام ۵ ساخته‌اید وارد شوید. نشانی دامنهٔ API صفحهٔ ورود مدیر ندارد. پاسخ فرانت و API را بررسی کنید.
2. روی نقطهٔ پایان HTTPS، TLS 1.0 و 1.1 و cipherهای CBC را غیرفعال کنید. برای Windows Server می‌توانید `configure-windows-tls.ps1` را ابتدا برای پیش‌نمایش و سپس در بازهٔ نگهداری با `-Apply` اجرا کنید. تنظیمات ابر آروان را در پنل آن انجام دهید.
3. متغیرهای موقت نشست نصب را پاک کنید:

```
Remove-Item
Env:INOGEN_TARGET_CONNECTION,Env:INOGEN_TARGET_ALLOWED_SERVER,Env:INOGEN_TARGET_ALLOWED_DATABASE -
ErrorAction SilentlyContinue
```