

Einrichtung vom ServiceOutside

Der ServiceOutside verwendet die Technologien vom .NET 6.0 Framework und ist auf einem Windows Server mit IIS (Internet Information Services) in einer DMZ zu hosten. Der Server vom ServiceOutside darf keinen Zugriff zum Intranet haben. Der Server soll mit einer Public Domain (S. Liste der möglichen Domains) vom Internet über HTTPS Protokoll erreichbar sein. Es ist wichtig, dass der Server für das HTTPS Protokoll ein autorisiertes und gültiges SSL-Zertifikat verwendet. Ein Self-Sign-Zertifikat ist nicht geeignet. Da der ServiceOutside für die interne Datenspeicherung eine MySQL Datenbank benötigt, muss auf demselben Server ein MySQL Server installiert und konfiguriert werden. Bitte ersetzen Sie die in der Doku verwendeten IP-Adressen/Hostnames und Domains mit Ihren echten Daten. Der Connection String zur MySQL-Datenbank und das Kennwort vom SMTP-Server sollen in appsettings.json verschlüsselt gespeichert werden. Für die Verschlüsselung der Daten in der appsettings.json verwenden Sie bitte die PasswortEncryptor.exe.

Empfohlene Konfiguration des Servers

| | |
|-----|------------------------|
| CPU | >= 8 CPU |
| RAM | >= 16 GB |
| SSD | >= 512 GB |
| OS | Windows Server >= 2019 |
| IIS | >= 10 |

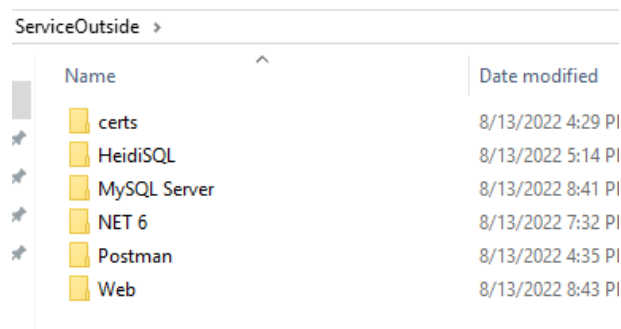
Inhalt der ServiceOutside1_0.zip Datei

Die Zip Datei „**ServiceOutside1_0.zip**“ enthält alle erforderlichen Dateien zum Installieren und Einrichten vom ServiceOutside.

1. Das Verzeichnis „**Web**“ enthält die Dateien für den Webserver, der in IIS gehostet wird
2. Das Verzeichnis „**MySQL Server**“ enthält die Installationsdatei „mysql-installer-community-8.0.30.0“ für den MySQL Server.

Das MySQL Schema für den ServiceOutside wird automatisch von der Applikation angelegt. Dafür soll nur in der Konfigurationsdatei vom ServiceOutside die Verbindungszeichenfolge hinterlegt werden. (S. appsettings.json)

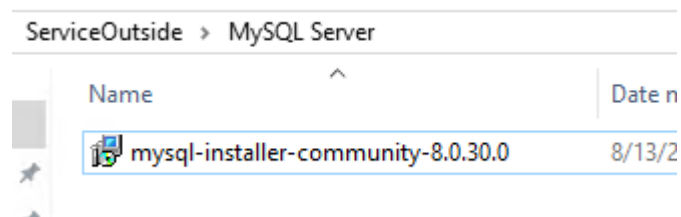
3. Das Verzeichnis „**HeidiSQL**“ enthält eine Anwendung „**heidisql.exe**“ mit der man die Verbindung zum MySQL Server testen kann.
4. Das Verzeichnis „**Postman**“ enthält eine Anwendung mit der man die Installation und Einrichtung vom ServiceOutside testen kann.
5. Das Verzeichnis „**certs**“ enthält die Zertifikate, die für die PUSH-Benachrichtigungen von IOS und Android Geräte verwendet werden. Bitte kopieren Sie das gesamte Verzeichnis „**certs**“ nach „**C:\certs**“ und passen Sie die Berechtigungen für den Webserver-Benutzer (**IIS_IUSRS**) so an, dass er die Zertifikate aus dem Verzeichnis „**C:\certs**“ lesen darf.
6. Das Verzeichnis „**NET 6**“ enthält die Installationsdatei vom .NET Framework 6.0.8



| Name | Date modified |
|--------------|-------------------|
| certs | 8/13/2022 4:29 PI |
| HeidiSQL | 8/13/2022 5:14 PI |
| MySQL Server | 8/13/2022 8:41 PI |
| NET 6 | 8/13/2022 7:32 PI |
| Postman | 8/13/2022 4:35 PI |
| Web | 8/13/2022 8:43 PI |

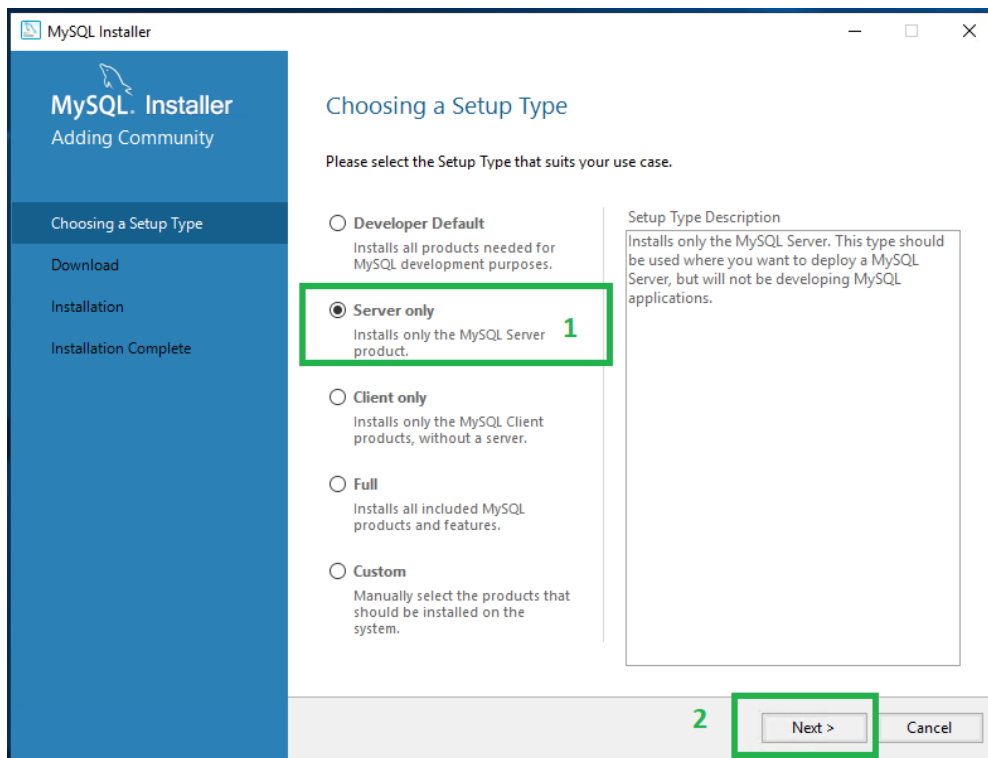
Installation und Einrichtung vom MySQL Server

1. Zum Installieren vom MySQL Server, gehen Sie bitte ins Verzeichnis „**MySQL Server**“ und führen Sie dort die Installationsdatei „**mysql-installer-community-8.0.30.0.exe**“ aus.

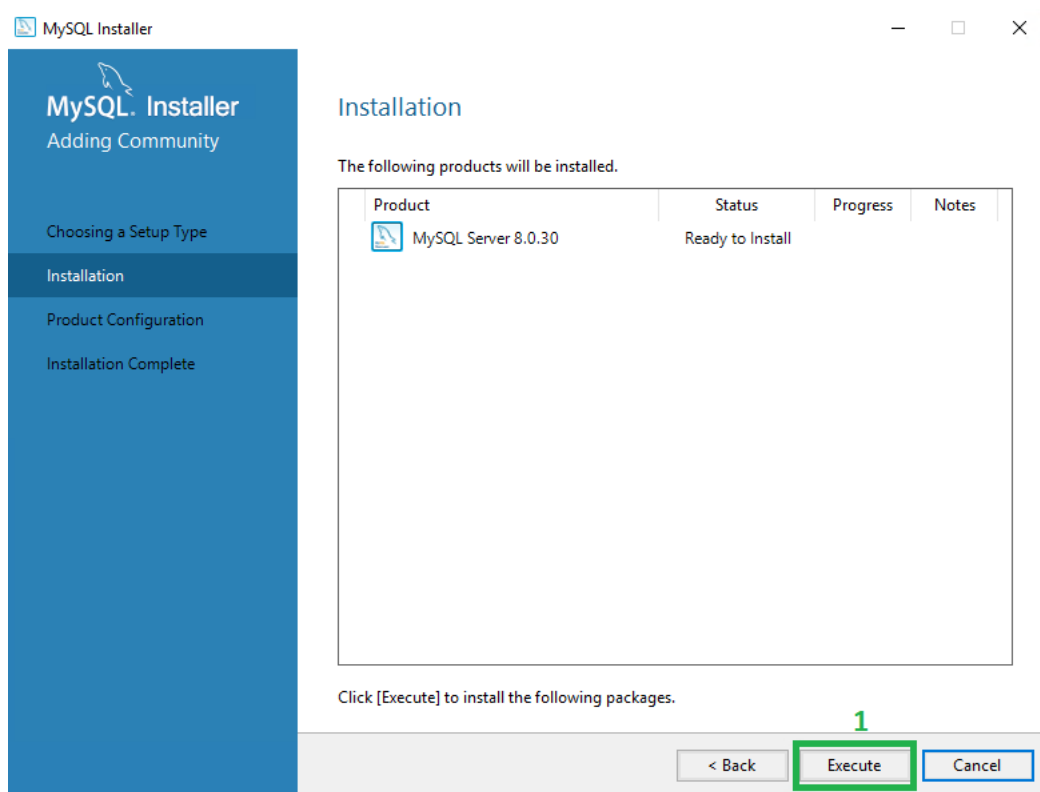


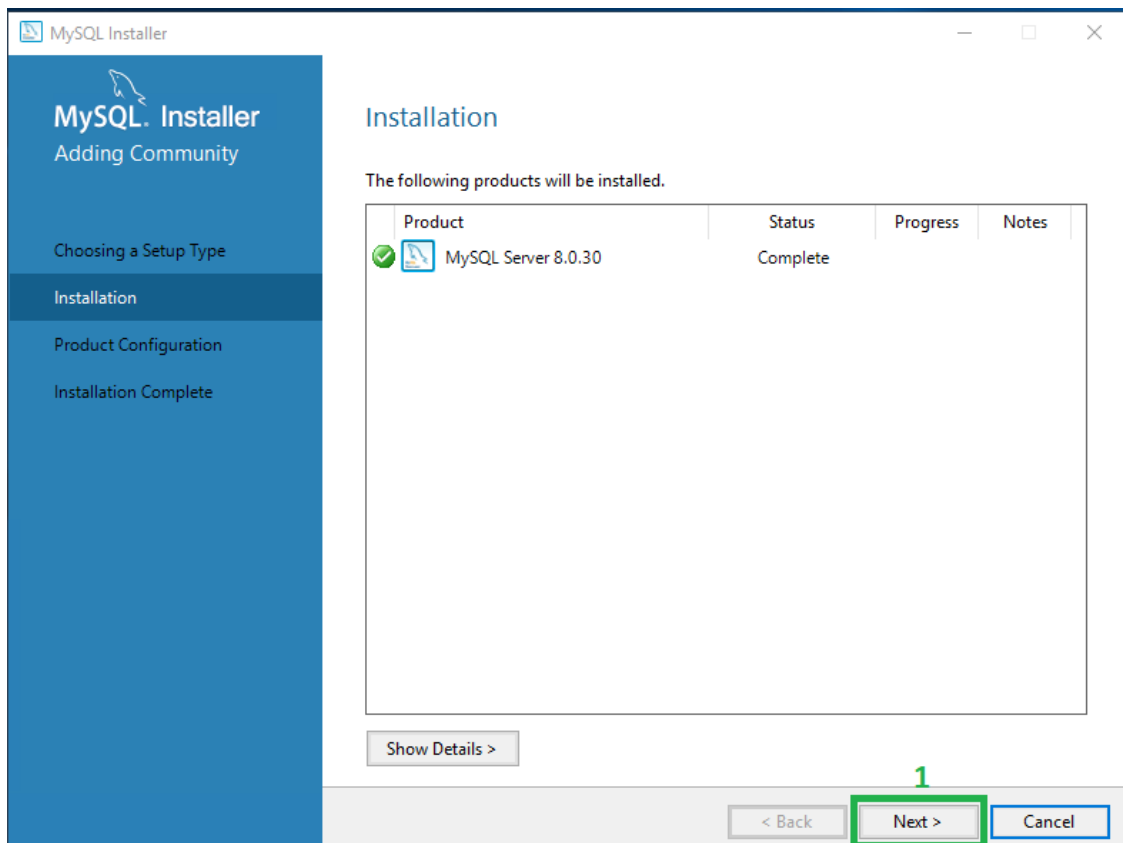
| Name | Date n |
|------------------------------------|--------|
| mysql-installer-community-8.0.30.0 | 8/13/2 |

2. Im MySQL Installer wählen Sie im Bereich „**Choosing a Setup Type**“ den Eintrag „**Server only**“ aus und klicken Sie anschließend auf „**Next**“.

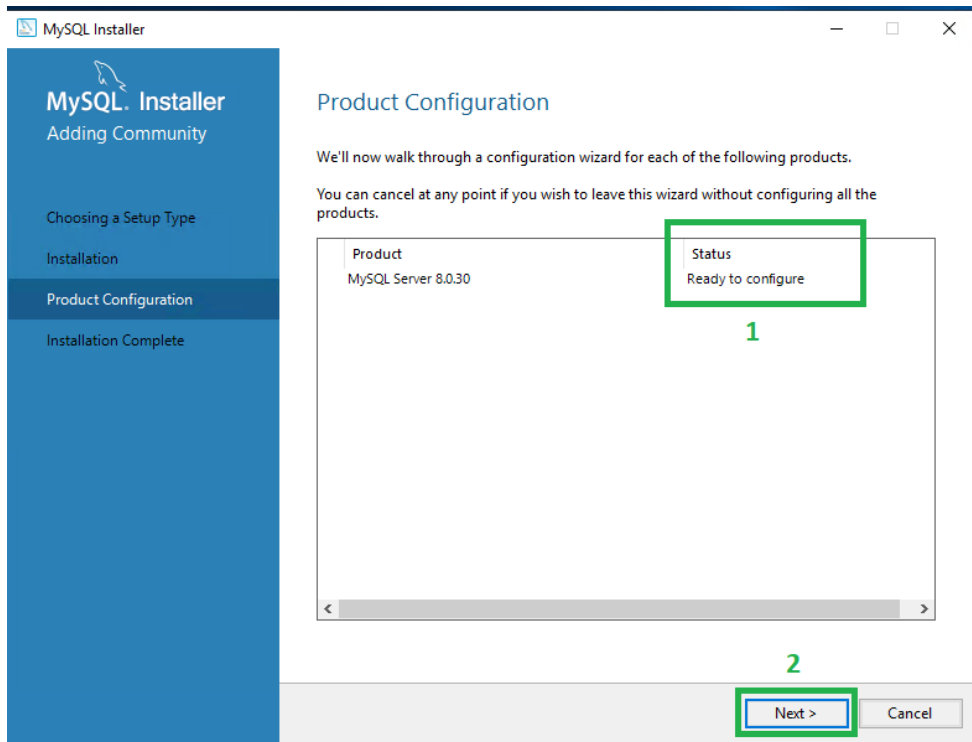


3. In der Maske „**Installation**“ klicken Sie auf „**Execute**“. Nach dem Abschluss des Installationsvorgangs klicken Sie auf „**Next**“.

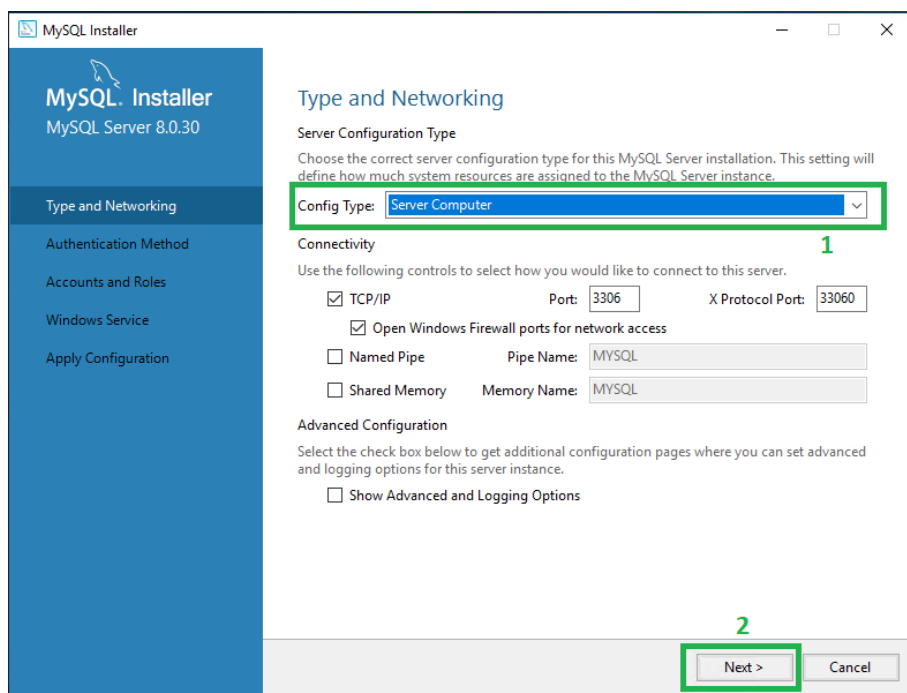




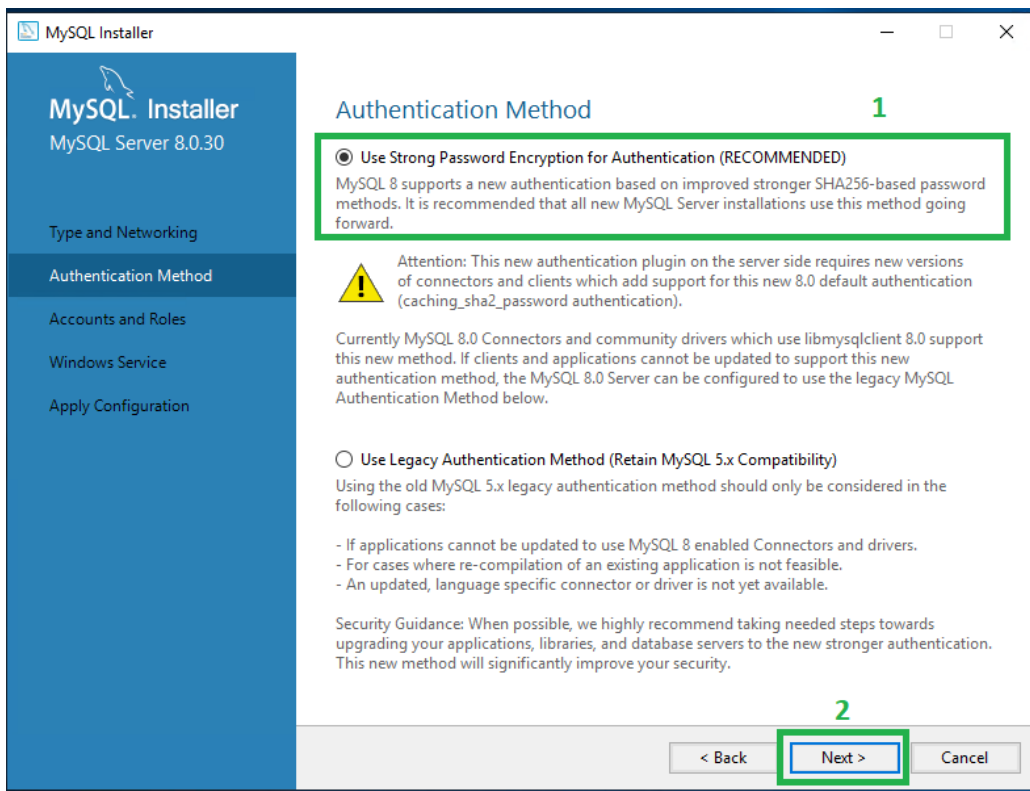
4. Sollte der Server alle erforderlichen Voraussetzungen für den MySQL Server erfüllen, zeigt die Maske „**Product Configuration**“ den **Status „Ready to configure“** an. Sollte bei der Installation die Voraussetzungen nicht erfüllt sein, zeigt die Maske die erforderlichen Schritte zur Beseitigung der Fehler an. Bitte zuerst alle Fehler korrigieren und anschließend auf „**Next**“ klicken.



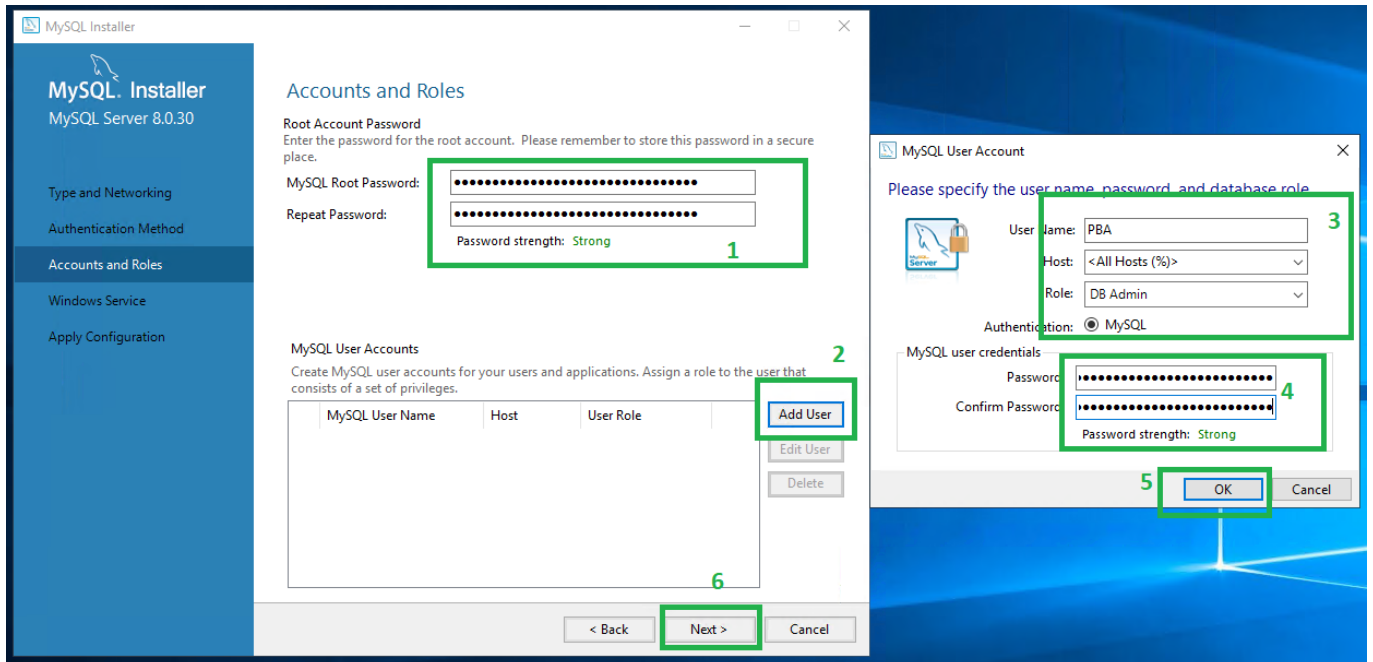
5. In der Maske „**Type and Networking**“ wählen Sie bitte unter **Config Type** den Eintrag „**Server Computer**“ aus und klicken Sie anschließend auf „**Next**“.



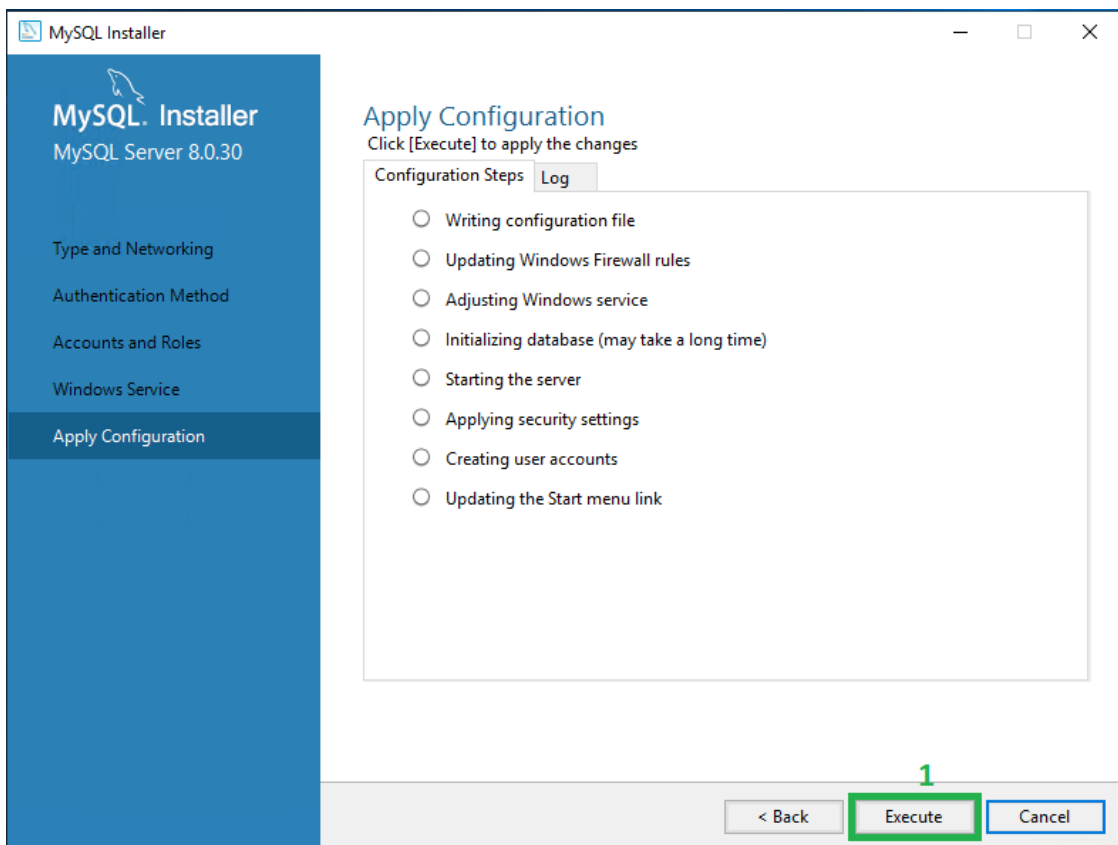
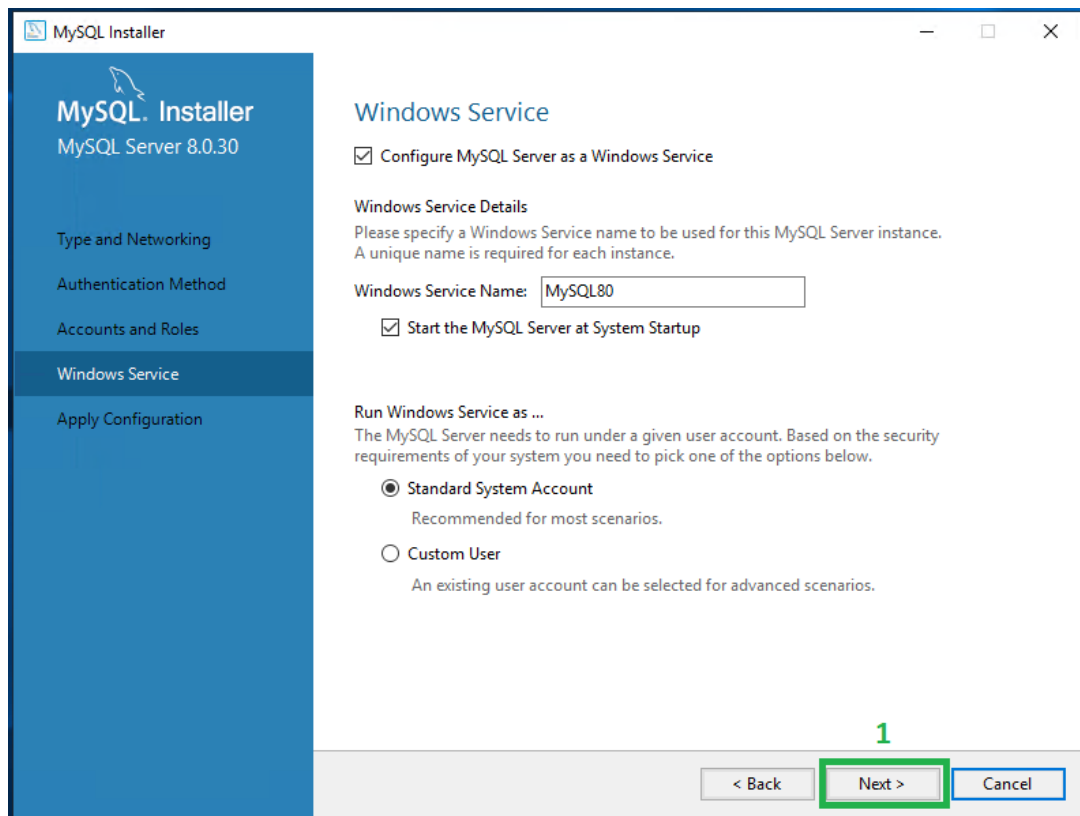
6. In der nächsten Maske „**Authentication Method**“ wählen Sie die Option „**Use Strong Password Encryption for Authentication (RECOMMENDED)**“ aus und klicken Sie auf „**Next**“.



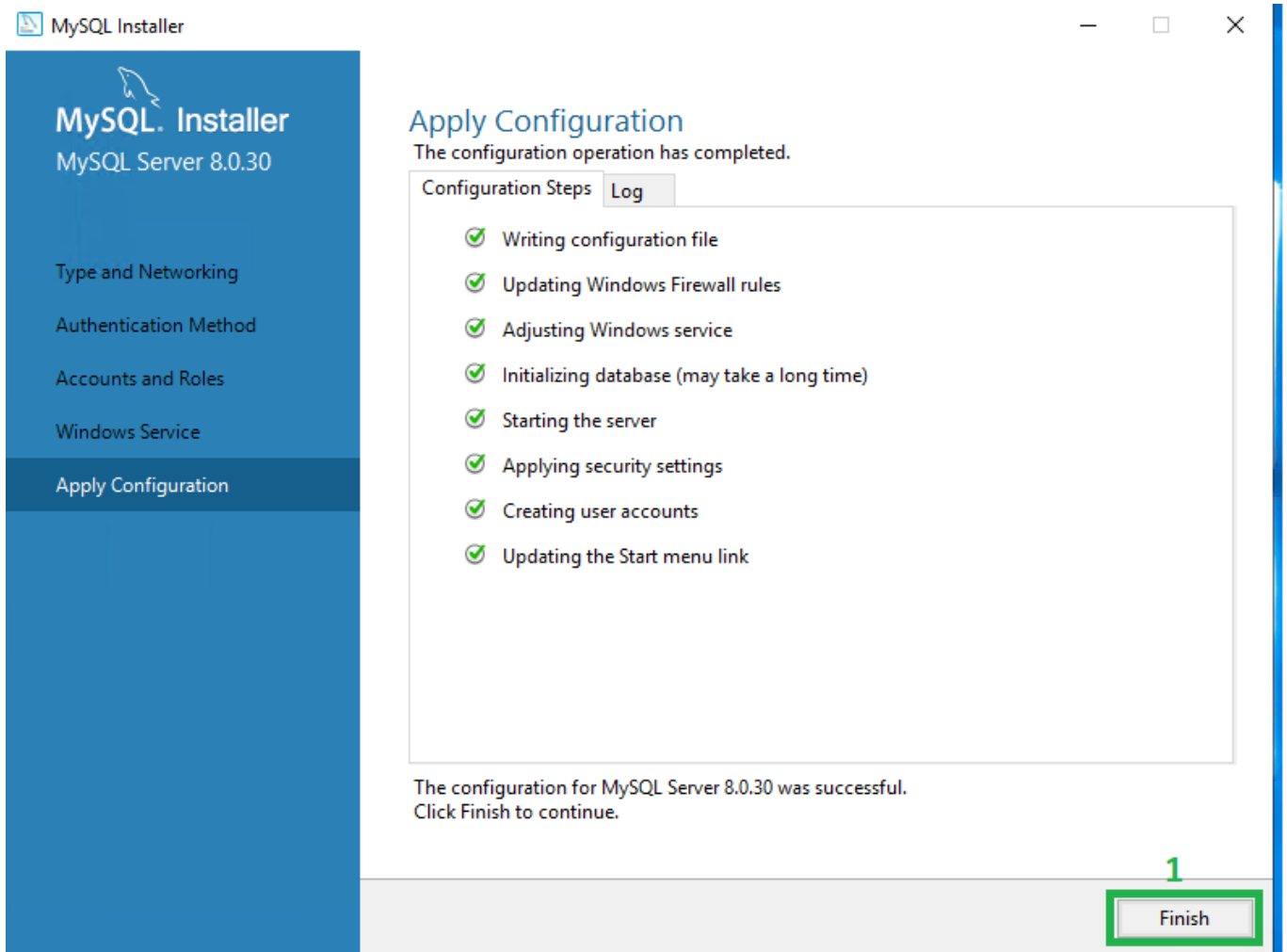
7. In der Maske „Accounts and Roles“ definieren Sie bitte ein starkes Passwort für den „Root“ Benutzer. Legen Sie bitte zusätzlich für den Webserver einen neuen Benutzer mit der Rolle „DB Admin“ und einem starken Passwort an.



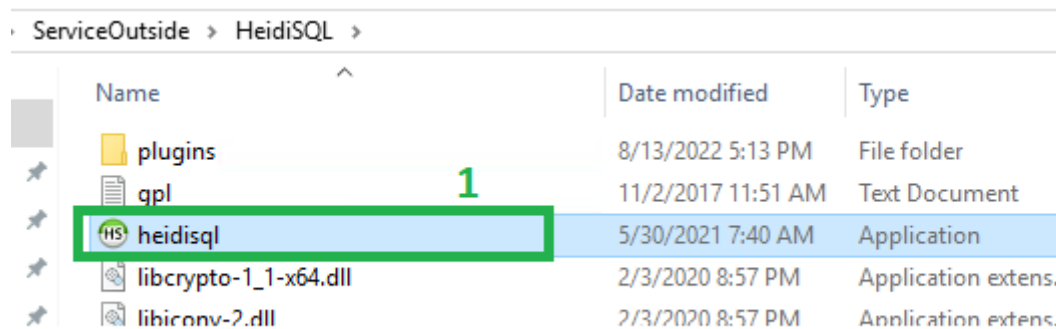
8. In der nächsten Maske „Windows Service“ starten Sie nun den MySQL-Service mit dem Klick auf „Next“ und zum Schluss auf „Execute“



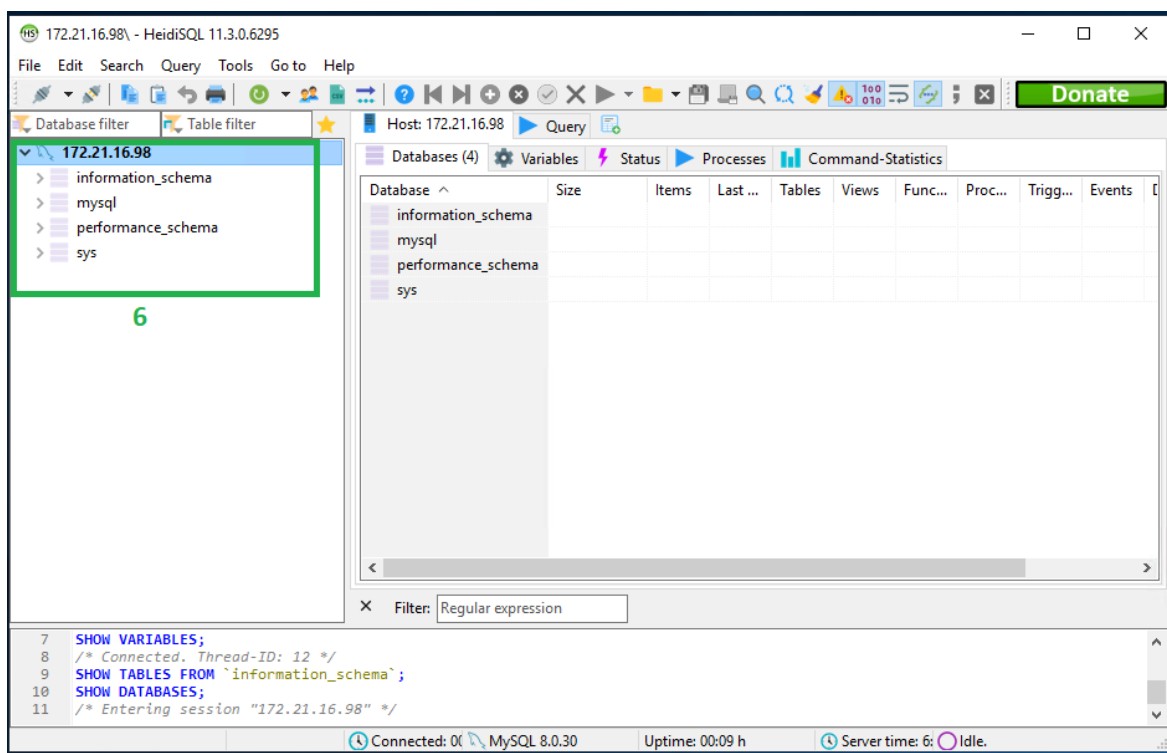
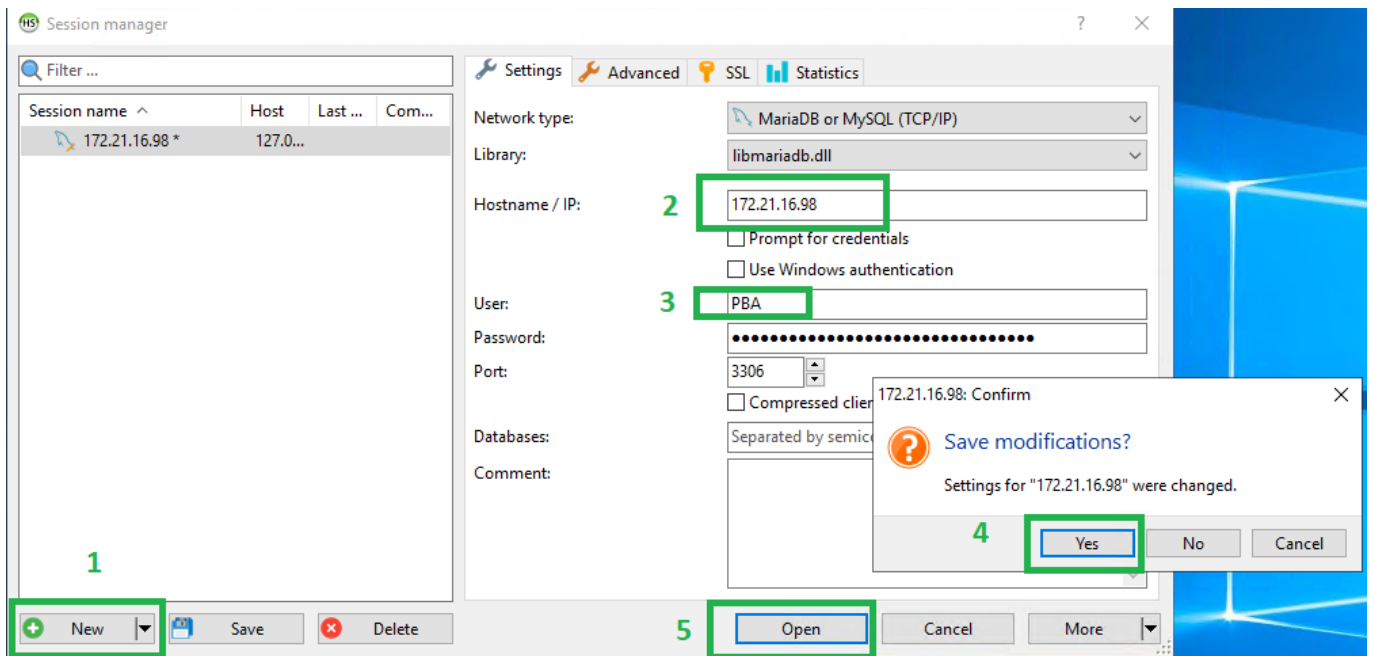
9. Sollte die Installation vom MySQL Server erfolgreich sein, schließen Sie die Installation mit dem Button „**Finish**“ ab.



10. Zur Prüfung der Datenbank Verbindung, führen Sie bitte die Anwendung „**heidisql.exe**“ im Verzeichnis „**HeidiSQL**“ aus.



Nun verbinden Sie sich mit dem Benutzer (kein Root Benutzer) zum MySQL Server.



Ist die Verbindung zum MySQL Server erfolgreich, so sehen Sie in der „HeidiSQL“ auf der linken Seite verschiedene Datenbanken wie z.B. „mysql“, „information_schema“, etc...

Wichtig: Da der ServiceInside zu diesem MySQL Server auch den Zugang haben muss, soll der MySQL Server die Anmeldungen über die TCP/IP Verbindungen zulassen.

Für die Zulassung der Anmeldung über die TCP/IP am MySQL Server, muss in der MySQL Konfigurationsdatei „my.ini“ im Bereich [mysqld] den Listener Eintrag angepasst werden.

Die Konfigurationsdatei „my.ini“ vom MySQL Server befindet sich auf einem Windows Server unter: „C:\ProgramData\MySQL\MySQL Server XX\my.ini“

Dort ist der folgende Eintrag im Bereich [mysqld] zu setzen:

The TCP/IP Port the MySQL Server will listen on

port=3306

bind-address = IP Adresse des Servers

mysqlx-bind-address = IP Adresse des Servers

The image shows a Windows File Explorer window displaying the path C:\ProgramData\MySQL\MySQL Server 8.0. The file my.ini is selected. Below it, a Notepad window is open, showing the contents of the my.ini file. The [mysqld] section is highlighted, and the following configuration is visible:

```
[mysqld]
# The next three options are mutually exclusive to SERVER_PORT below.
# skip-networking
# enable-named-pipe
# shared-memory

# shared-memory-base-name=MYSQL

# The Pipe the MySQL Server will use.
# socket=MYSQL

# The access control granted to clients on the named pipe created by the MySQL Server.
# named-pipe-full-access-group=

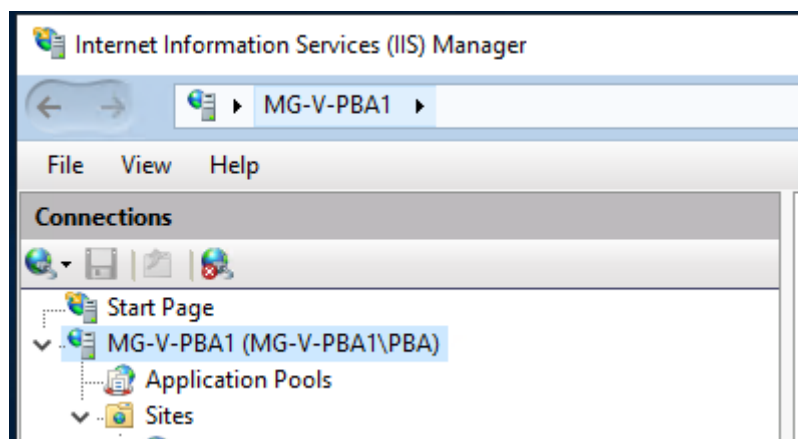
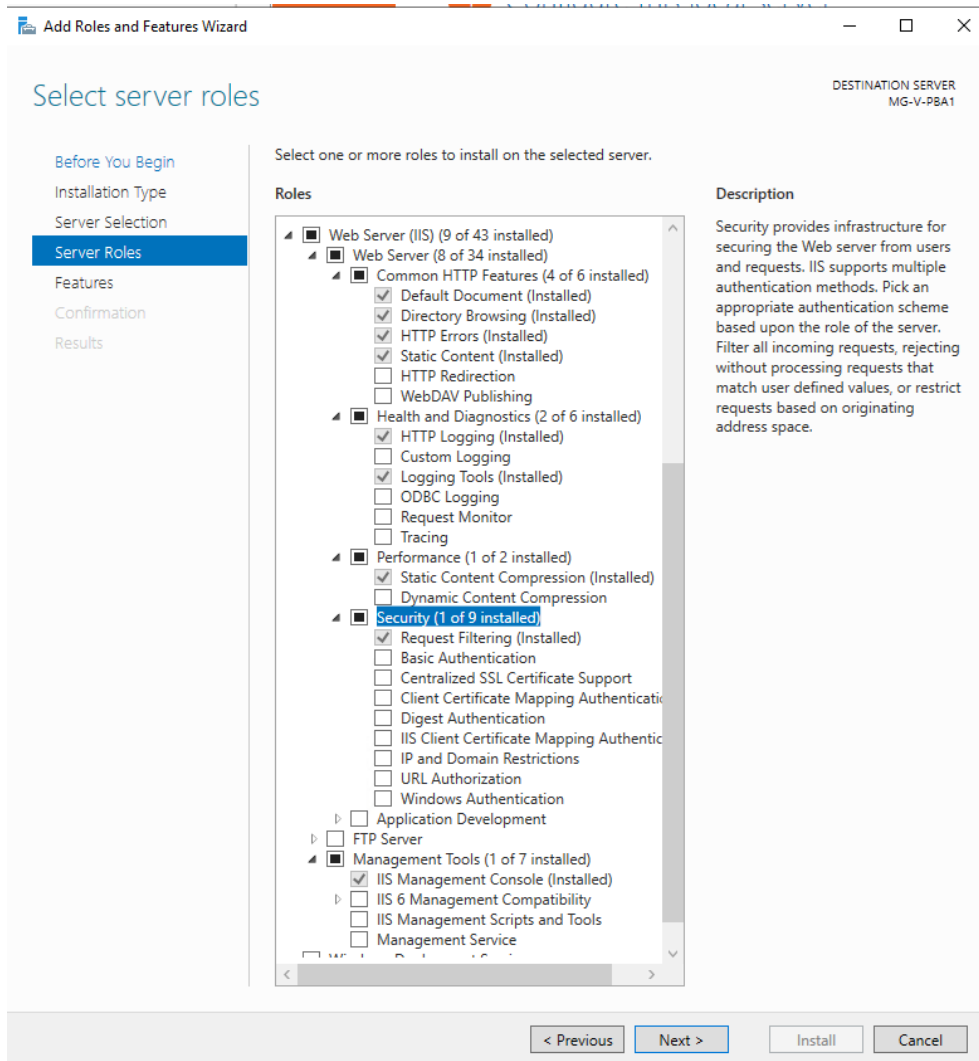
# The TCP/IP Port the MySQL Server will listen on
port=3306
bind-address = 172.21.16.98
mysqlx-bind-address = 172.21.16.98
```

Nach der Anpassung der MySQL Konfigurationsdatei „my.ini“, muss der MySQL Service neu gestartet werden

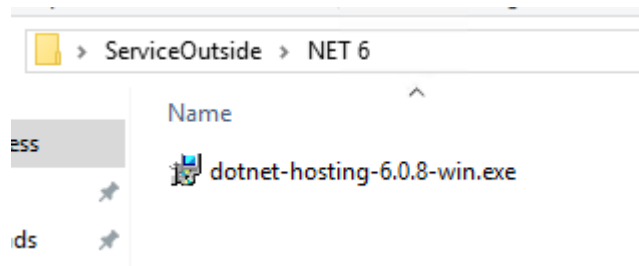
The image shows the Windows Services console. The MySQL80 service is selected, and the context menu is open. The 'Restart' option is highlighted, indicating that the service is being restarted.

Installation und Einrichtung vom Webserver

1. Aktivieren Sie nun den Webserver(IIS) in „Roles and Features“ vom System und rufen Sie anschließend den IIS Manager auf. Falls in IIS eine Default Site bereits vorhanden ist, löschen Sie bitte diese zuerst, bevor Sie mit der Konfiguration vom ServiceOutside fortsetzen.

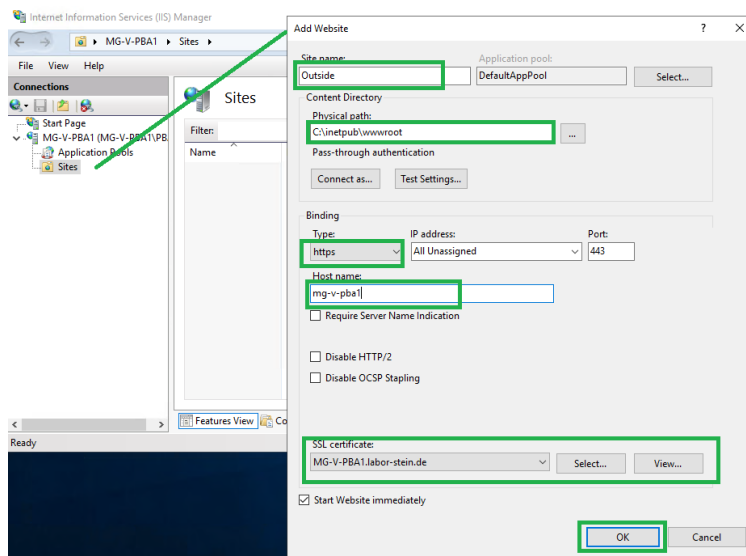


2. Für den Webserver soll zuerst das NET 6 Framework installiert werden. Zum Installieren vom NET 6 Framework führen Sie bitte die Installationsdatei „**dotnet-hosting-6.0.8-win.exe**“ im Verzeichnis „**NET 6**“ aus.



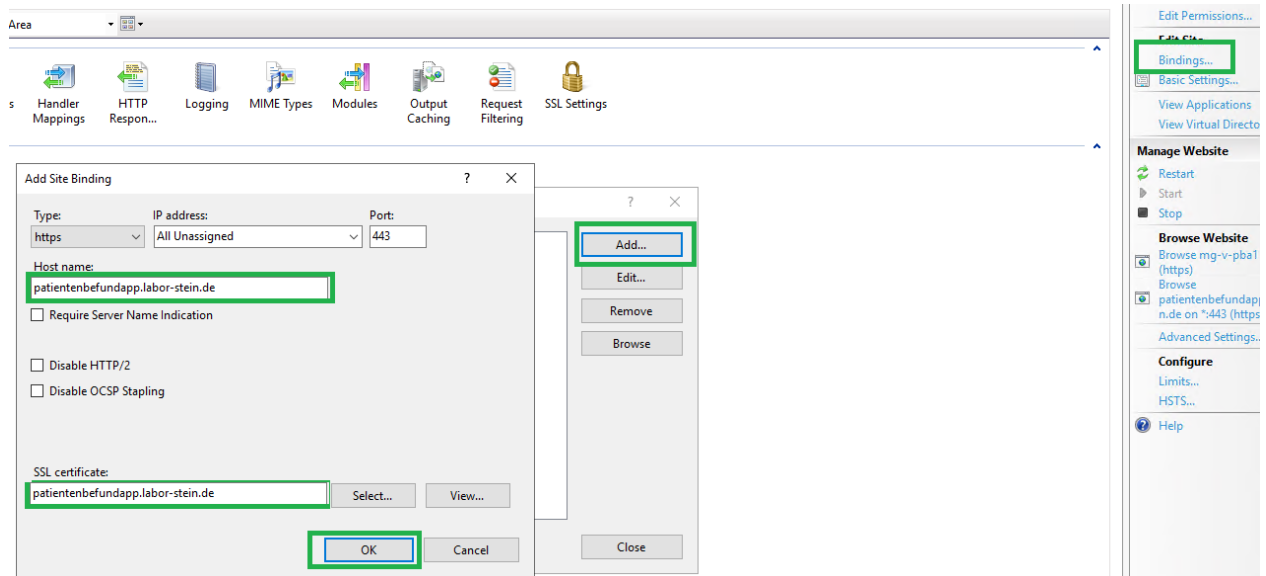
3. Kopieren Sie die Dateien aus dem Verzeichnis „**Web**“ nach **C:\inetpub\wwwroot**.
4. Legen Sie nun eine neue Seite im IIS Manager an

- a: Geben Sie als Name der Seite „**Outside**“ ein
- b: Wählen Sie als „**Application Pool**“ „**DefaultAppPool**“ aus
- c: Wählen Sie als physikalischen Pfad das Verzeichnis „**C:\inetpub\wwwroot**“ aus
- d: Wählen Sie als Standard Binding das https Protokoll (443) aus und tragen Sie als Hostname den Namen des Servers ein. Später wird eine weitere Binding für die public Domain definiert.

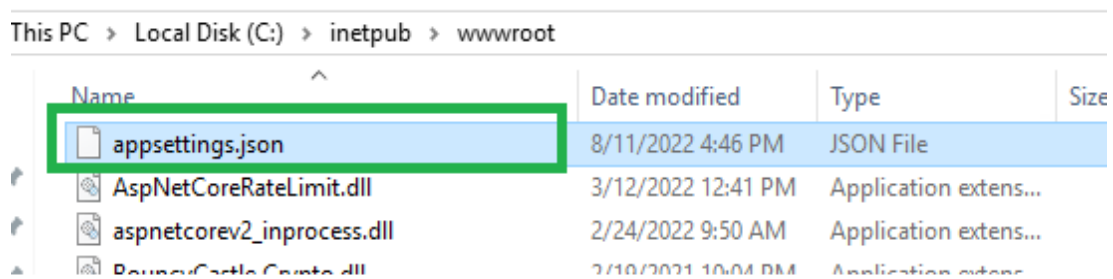


Wichtig: Es muss ein gültiges Zertifikat verwendet werden.

5. Tragen Sie nun eine weitere Binding für die public Domain (S. Liste der verfügbaren Domains) ein. Es ist wichtig, dass für die public Domain ein gültiges Zertifikat verwendet wird.



- Öffnen Sie die „**appsettings.json**“ Datei im Verzeichnis „**C:\inetpub\wwwroot**“, um den ServiceOutside vollständig zu konfigurieren.



- Ergänzen Sie die WhiteListe in der Konfigurationsdatei mit den IP-Adressen vom ServiceInside und ServiceOutside.

```

{
  "Log": {
    "Type": "DEBUG",
    "Path": "c:\\tmp\\outside",
    "SmtpServer": "172.21.101.88",
    "SmtpPort": 25,
    "SmtpSSL": false,
    "SmtpSenderEmail": "ServiceOutside@labor-stein.de",
    "SmtpSenderName": "ServiceOutside",
    "SmtpRecipients": "iabetschkhrischwili@labor-stein.de"
  },
  "IpRateLimiting": {
    "EnableEndpointRateLimiting": true,
    "StackBlockedRequests": false,
    "RealIPHeader": "X-Real-IP",
    "ClientIdHeader": "X-ClientId",
    "HttpStatusCode": 429,
    "IpWhitelist": [ "127.0.0.1", "::1", "IP vom ServiceInside", "IP vom ServiceOutside" ],
    "GeneralRules": [
      {
        "Endpoint": "*",
        "Period": "1m",
        "Limit": 20
      }
    ]
  }
}

```

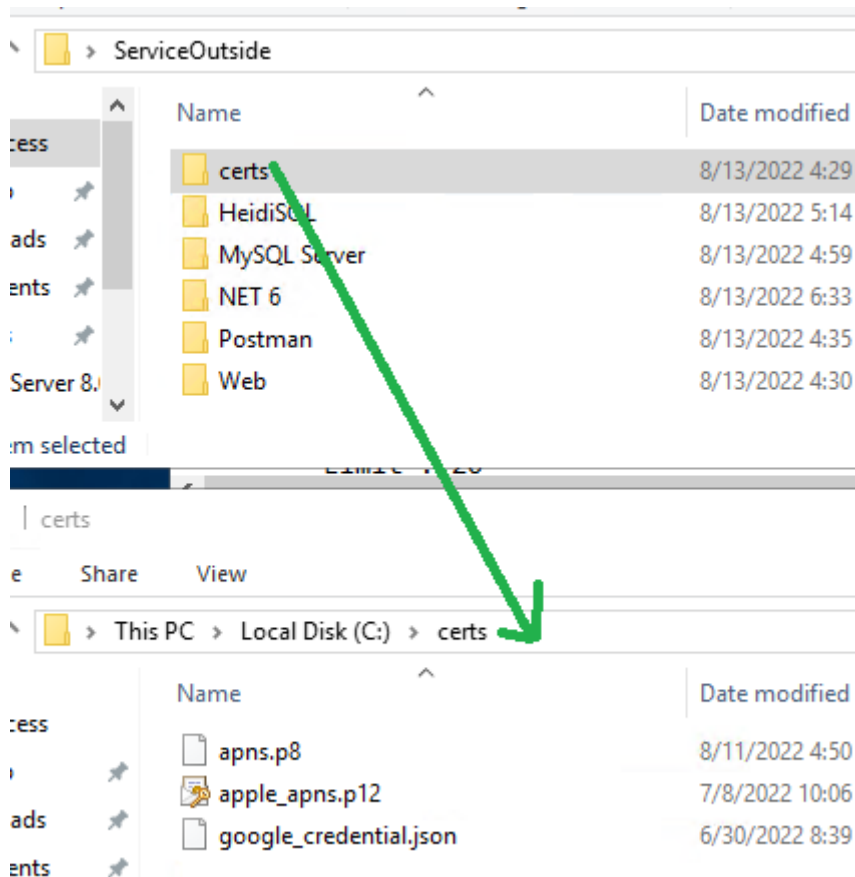
- Tragen Sie in den Feldern „**ServiceInsideIP**“ und „**ServiceInsideURL**“ die IP und die URL vom ServiceInside ein

```

    ],
    "ServiceInsideIP": "172.21.16.106",
    "ServiceInsideURL": "https://172.21.16.106",
    "ConnectionStrings": {
      "default": "prod",
    }
  }
}

```

9. Für die PUSH Benachrichtigungen kopieren Sie bitte das gesamte Verzeichnis „certs“ mit den Zertifikaten nach „c:\certs“ und passen Sie die Pfade in der „appsettings.json“ Datei bei „PushNotifications“ an.



```

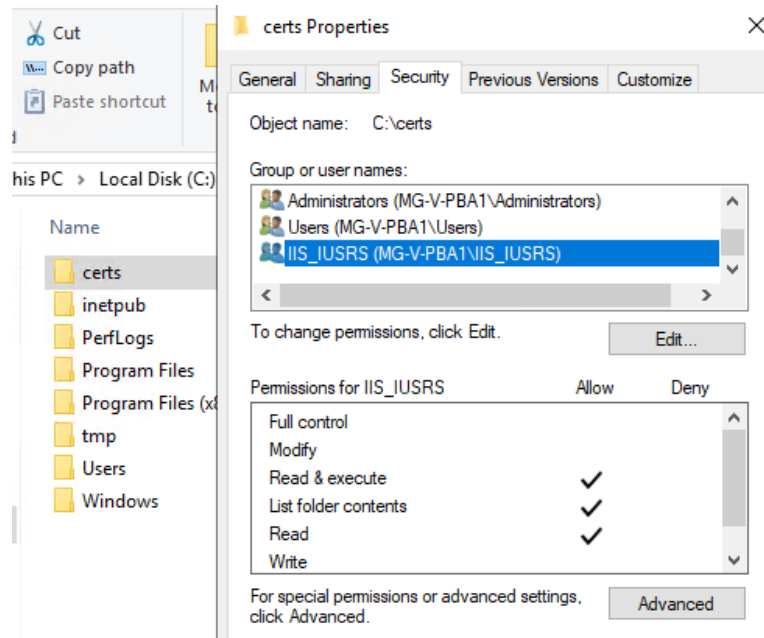
"PushNotifications": {
  "APNS": {
    "Type": "PRODUCTION",
    "BundleId": "de.labor-stein.Befund",
    "Cert": "C:\\\\certs\\apns.p8",
    "KeyId": "938D85LA3G",
    "TeamId": "9239XBB72R"
  },
  "GOOGLE": {
    "CredentialJson": "C:\\\\certs\\google_credential.json"
  }
}

```

Wichtig: Der WebServer Benutzer(IIS_IUSRS) soll berechtigt sein die beiden Zertifikate zu lesen. Desweiteren sollen folgende Verbindungen nach außen für die PUSH-Benachrichtigungen erlaubt sein:

oauth2.googleapis.com:443 (GOOGLE)

api.push.apple.com:443 (IOS)



10. Für die Datenbankverbindung tragen Sie bitte in der Konfigurationsdatei „**appsettings.json**“ unter „**ConnectionString**“ bei default „**prod**“ und im prod ersetzten Sie die Daten durch die echten Daten von Ihrem MySQL Server.

```
''  
"ServiceInsideIP": "172.21.16.106",  
"ServiceInsideURL": "https://172.21.16.106",  
"ConnectionStrings": {  
  "default": "prod",  
  "prod": "Server=myServerAddress;Database=myDataBase;Uid=myUsername;Pwd=myPassword",  
  "dev": "",  
  "test": ""  
}.  
}
```

Verschlüsselter ConnectionString

```
"ConnectionStrings": {  
  "default": "dev",  
  "prod": "XHQS8gr8XSwdVnoDZ04Ha/wZe10/XVr5Wkc1TjcKe/Z3aW0MbgKQGZVhRTHXZkv4mkkxv9z3PK7p0IMAM3J+ta5d6kid8"
```

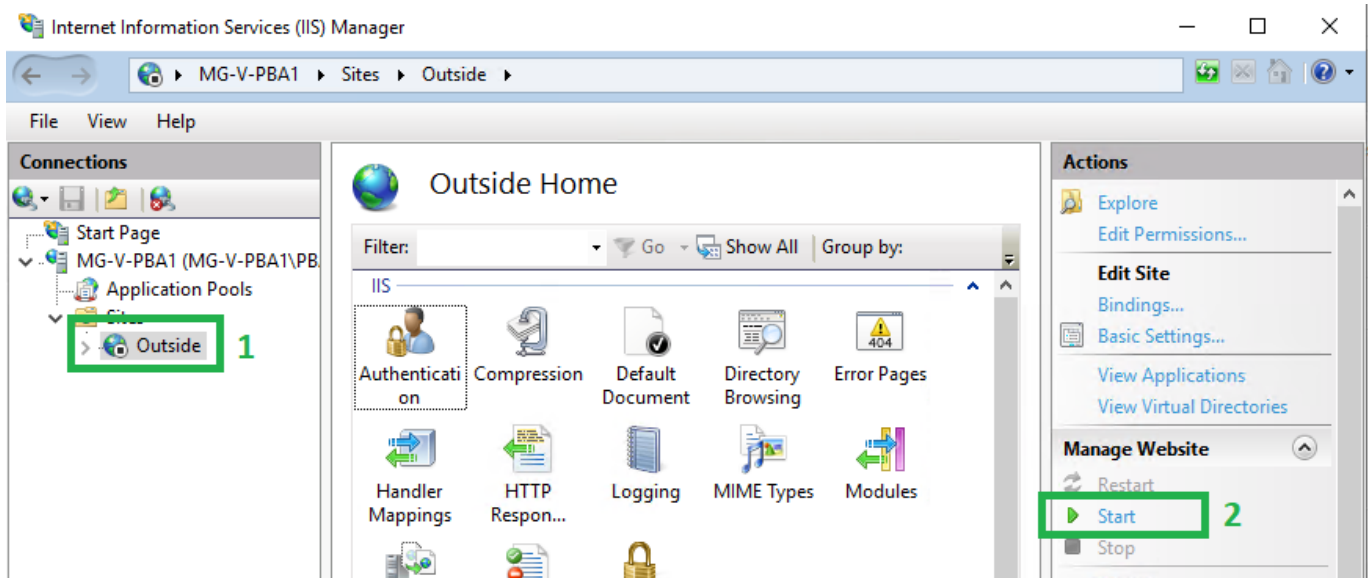
11. Damit der Server die E-Mails versenden kann, soll in der Konfigurationsdatei „**appsettings.json**“ ein SMTP-Server konfiguriert werden. Der Versand der E-Mails werden für die Logs der Applikation und die Anfrage (Account löschen, etc..) der Patienten verwendet. Es ist wichtig, dass in Smt recipients die Mitarbeiter definiert werden, die sowohl über die kritischen Anwendungsfehler als auch über die Anfragen der Patienten informiert werden sollen.

```
"Log": {
  "Type": "DEBUG",
  "Path": "c:\\tmp\\outside",
  "SmtpServer": "172.21.101.88",
  "SmtpPort": 25,
  "SmtpSSL": false,
  "SmtpSenderEmail": "ServiceOutside@labor-stein.de",
  "SmtpSenderName": "ServiceOutside",
  "SmtpRecipients": "iabetschkhrischwili@labor-stein.de"
},
```

Verschlüsseltes SmtPassword

```
"Log": {
  "Type": "DEBUG",
  "Path": "c:\\tmp\\outside",
  "SmtpServer": "172.21.101.88",
  "SmtpPort": 25,
  "SmtpSSL": false,
  "SmtpUsername": "SmtpUser",
  "SmtpPassword": "yd/KLV70/pXzyHaveZM3b01CfcVklFLkDVHXYU0GrQv6B+w=",
  "SmtpSenderEmail": "ServiceInside@labor-stein.de",
  "SmtpSenderName": "ServiceInside",
  "LogsRecipients": "iabetschkhrischwili@labor-stein.de",
  "CustomerRequestsRecipients": "empfaenger@labor-stein.de"
},
```

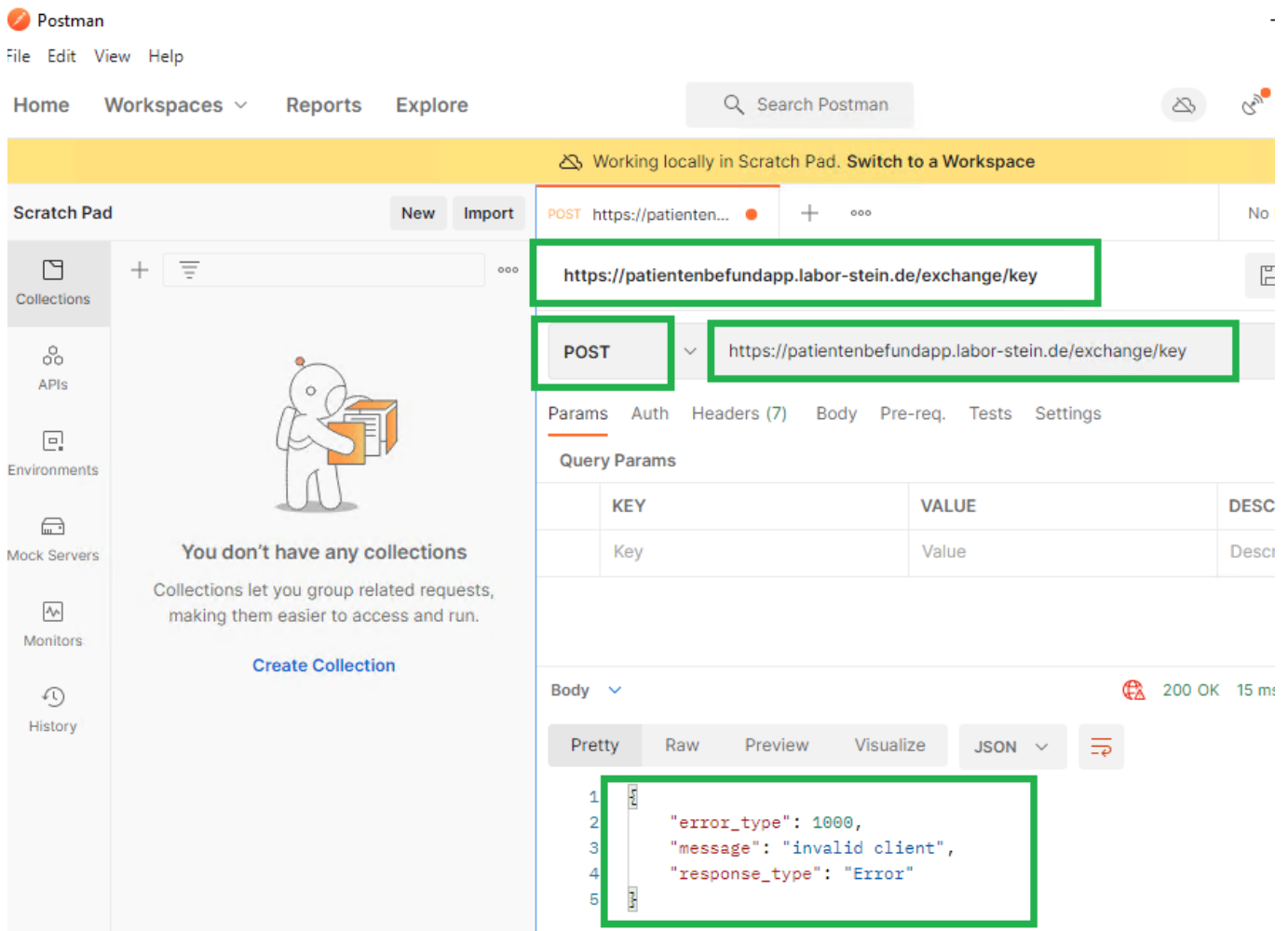
12. Starten Sie nun die neu angelegte Seite „Outside“ im IIS Manager.



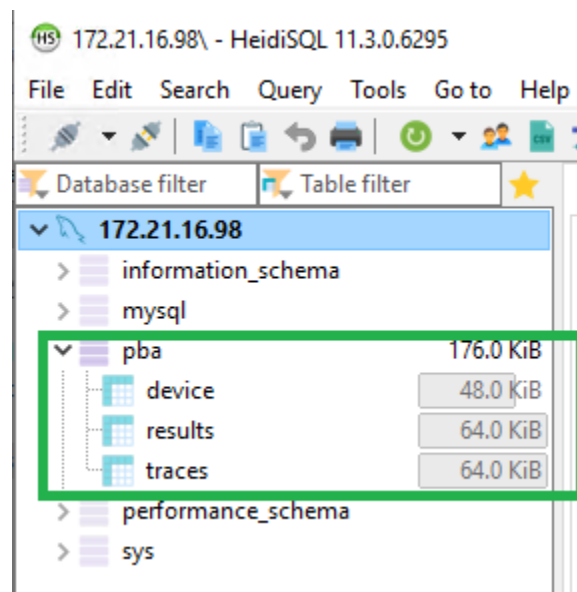
13. Zum Testen vom ServiceOutside führen Sie bitte die Anwendung „**Postman.exe**“ im Verzeichnis „**Postman**“ aus. Anschließend führen Sie bitte in „**Postman**“ eine HTTPS POST-Abfrage mit der URL „public domain“/exchange/key aus

z.B: public domain: patientenbefundapp.labor-stein.de

Auszuführende URL: patientenbefundapp.labor-stein.de/exchange/key



Sollte der Webserver eine Antwort mit dem `error_type: 1000` „invalid client“ zurück liefern, so wurde der ServiceOutside erfolgreich eingerichtet. Das Weiteren sollte der ServiceOutside nach der ersten erfolgreichen Abfrage selbständig das Schema in der MySQL Datenbank angelegt haben.



Sollte der ServiceOutside bei der Abfrage nicht korrekt reagiert haben, aktivieren Sie bitte in der Konfigurationsdatei „**appsettings.json**“ den **DEBUG** Log und legen Sie einen Pfad für die Protokollierung der Fehler fest. Der ServiceOutside protokolliert nun alle Abfragen mit den Fehlern in der Datei.

```
{
  "Log": {
    "Type": "DEBUG",
    "Path": "c:\\tmp\\outside",
    "SmtpServer": "172.21.101.88",
    "SmtpPort": 25,
    "SmtpSSL": false,
    "SmtpSenderEmail": "ServiceOutside@labor-stein.de",
    "SmtpSenderName": "ServiceOutside",
    "SmtpRecipients": "iabetschkhrischwili@labor-stein.de"
  },
}
```

Zur weiteren Recherche von Problemen kann auch in der „**C:\inetpub\wwwroot\web.config**“ Datei die Protokollierung der Console-Ausgabe aktiviert werden.



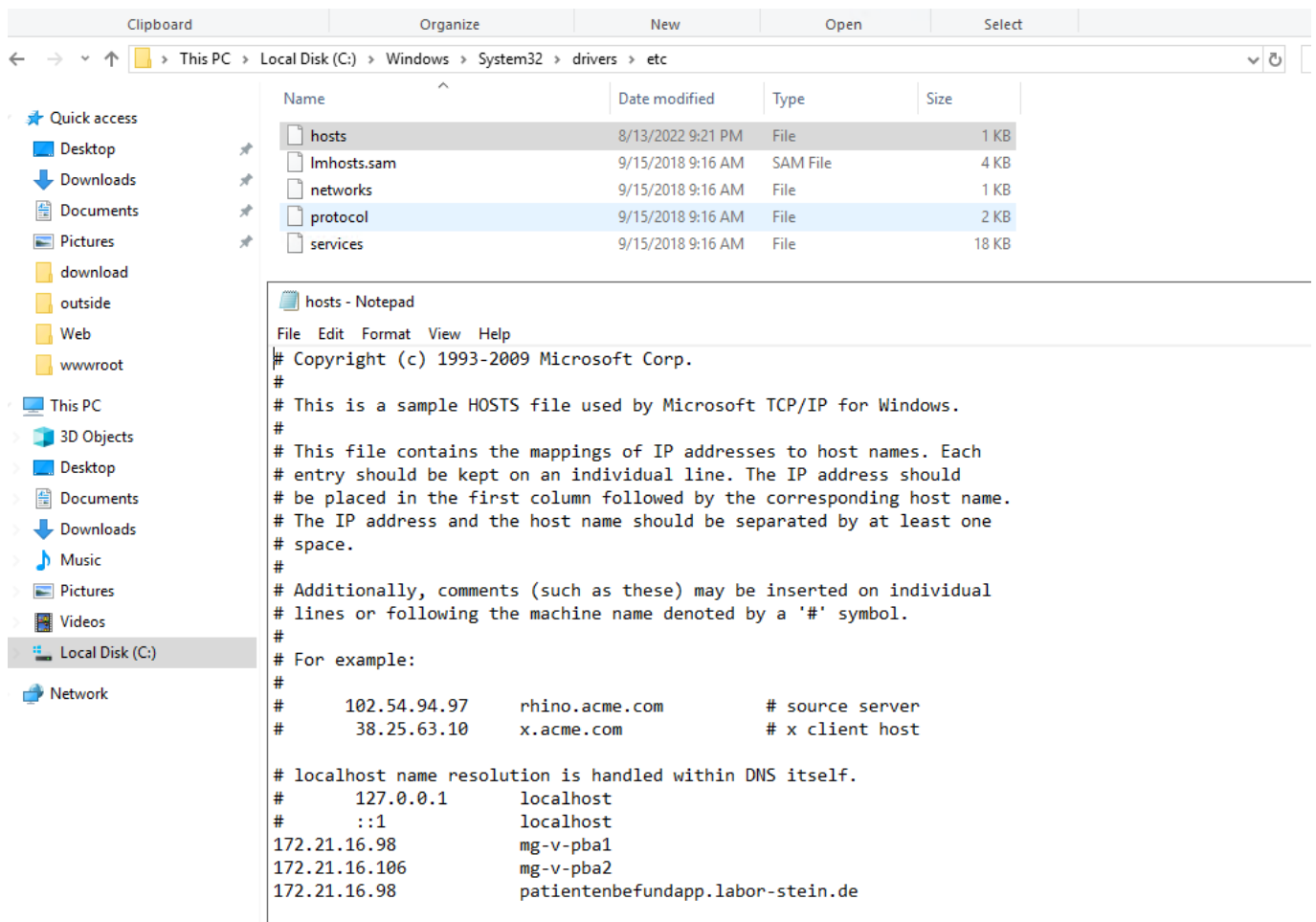
```
web.config - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <location path="." inheritInChildApplications="false">
    <system.webServer>
      <handlers>
        <add name="aspNetCore" path="*" verb="*" modules="AspNetCoreModuleV2" resourceType="Unspecified" />
      </handlers>
      <aspNetCore processPath=".\\ServiceOutside.exe" stdoutLogEnabled="true" stdoutLogFile="c:\\tmp\\logs.txt" hostingModel="inprocess" />
    </system.webServer>
  </location>
</configuration>
<!--ProjectGuid: 82019c47-9b6b-466a-ae18-c1d1d15441ca-->
```

Nach der erfolgreichen Installation vom ServiceOutside setzen Sie bitte den LOG Modus in der „**appsettings.json**“ auf ERROR, damit nur die Fehler protokolliert werden.

Fehlerbehebung

1. Falls der ServiceOutside nach der Installation auf die Test-Abfragen nicht reagiert, prüfen Sie bitte, ob der Webservice mit dem Hostname, den Sie in IIS als Binding angelegt haben erreichbar ist. Bitte beachten Sie, dass der Webservice nur über einen Hostnamen oder eine Domain aufgerufen werden kann. Ein Aufruf der Webservices über die IP ist nicht zugelassen, da ein SSL Zertifikat verwendet wird und dieses nur einen Hostname oder eine Domain verifizieren kann. Es ist wichtig, dass der Hostname des Servers auch die richtige IP-Adresse auflöst. Sollte ein DNS

Server nicht zentral vorhanden sein, tragen Sie bitte alle notwendigen IP-Adressen mit den zugehörigen Hostname in der lokalen hosts Datei ein.



The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Local Disk (C:) > Windows > System32 > drivers > etc'. The file list shows several files, with 'hosts' selected. A Notepad window titled 'hosts - Notepad' is open, displaying the contents of the hosts file. The text in the Notepad window is as follows:

```
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com             # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1             localhost
172.21.16.98           mg-v-pba1
172.21.16.106          mg-v-pba2
172.21.16.98           patientenbefundapp.labor-stein.de
```

Liste der verfügbaren Domains für OutsideService abhängig vom Labor

patientenbefundapp.labor-limbach.de

patientenbefundapp.mvz-labor-lb.de

patientenbefundapp.humangenetik-ulm.de

patientenbefundapp.labor-aachen.de

patientenbefundapp.mdi-limbach-berlin.de

patientenbefundapp.labor-cottbus.de

patientenbefundapp.laborpraxis-dessau.de

patientenbefundapp.labor-dortmund.de

patientenbefundapp.labordresden.de

patientenbefundapp.labor-erfurt.de

patientenbefundapp.labor-eveld.de
patientenbefundapp.mvz-clotten.de
patientenbefundapp.labor-limbach-hannover.de
patientenbefundapp.labor-hofheim.de
patientenbefundapp.laborvolkmann.de
patientenbefundapp.labor-leipzig.de
patientenbefundapp.labor-stein.de
patientenbefundapp.labor-limbach-muenchen.de
patientenbefundapp.labor-muenster.de
patientenbefundapp.labor-limbach-nuernberg.de
patientenbefundapp.labor-passau.de
patientenbefundapp.labor-gaertner.de
patientenbefundapp.medlabor.de
patientenbefundapp.laboraerzte-schweinfurt.de
patientenbefundapp.labor-schwerin.de
patientenbefundapp.labor-stralsund.de
patientenbefundapp.labor-suhl.de
patientenbefundapp.mlh.de
patientenbefundapp.medgen-mainz.de
patientenbefundapp.laborarztpraxis.de