Einrichtung vom ServiceInside

Der Servicelnside 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 Servicelnside darf keinen Zugriff zum Intranet haben. Darüber hinaus darf der Servicelnside nicht vom Internet erreichbar sein. Nur der ServiceOutside darf mit dem ServiceInside über das HTTPS Protokoll kommunizieren. Es ist wichtig, dass der ServiceOutside zuerst eingerichtet wird und erst danach kann der ServiceInside vollständig eingerichtet werden. Auf dem Server vom ServiceInside soll eine Freigabe mit einem lokalen Benutzer eingerichtet werden. In dieser Freigabe, sollen die Dateien vom LIS/MIRTH/etc... zur Steuerung der Backendservices gelesen und geschrieben werden. (S. Dokumentation über die LIS-Anbindung). 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 ServiceInside1_0.zip Datei

Die Zip Datei "ServiceInside1_0.zip" enthält alle erforderlichen Dateien zum Installieren und Einrichten vom ServiceInside.

- 1. Das Verzeichnis "**Web**" enthält die Dateien für den Webserver, der in IIS gehostet wird.
- 2. Das Verzeichnis "**HeidiSQL**" enthält eine Anwendung "**heidisql.exe**" mit der man die Datenbankverbindung zum MySQL Server testen kann.

- 3. Das Verzeichnis "**Postman**" enthält eine Anwendung mit der man die Installation und Einrichtung vom ServiceInside testen kann.
- 4. Das Verzeichnis "NET 6" enthält die Installationsdatei vom .NET Framework 6.0.8

Installation und Einrichtung vom Webserver

Bevor man mit der Installation und Einrichtung vom Webserver anfängt soll zuerst geprüft werden, ob der ServiceInside die MySQL-Datenbank vom ServiceOutside über die IP Adresse und Port erreichen kann. Zum Testen der Datenbankverbindung führen Sie bitte die Anwendung "**heidisql.exe**" im Verzeichnis "**HeidiSQL**" aus und verbinden Sie sich mit dem MySQL Server. (Der ServiceOutside muss zuerst eingerichtet werden)



Bession manager					? ×
C Filter				🖋 Settings 🎤 Advanced	SSL SSL SSL SSL SSL
Session name	Host	Last	Com	Network type:	NariaDB or MySQL (TCP/IP)
Ŋ 172.21.16.98 *	127.0			Library:	libmariadb.dll 🗸
				Hostname / IP: 2	172.21.16.98
					Prompt for credentials Use Windows authentication
				User: 3	PBA
				Password:	2206
				FOL.	Compressed clier 172.21.16.98: Confirm X
				Databases:	Separated by semice Save modifications?
				Comment:	Settings for "172.21.16.98" were changed.
1					4 Yes No Cancel
O New ▼	Save	8	Delete	5	Open Cancel More

Als nächstes prüfen Sie bitte, ob der ServiceOutside über das HTTPS Protokoll vom ServiceInside erreichbar ist. Dafür führen Sie bitte die Anwendung **"Postman.exe"** im Verzeichnis **"Postman"** aus und führen Sie anschließend in **"Postman"** die HTTPS POST-Abfrage mit der URL "Hostname vom ServiceOutside"/exchange/key aus:

z.B: Hostname vom ServiceOutside: mg-v-pba1 (Nur intern erreichbar)

Auszufuhrende URL: mg-v-pba1/exchange/key

🥖 Postman								
File Edit Vie	ew Help							
Home V	Norkspaces V Reports Explore			Q Search	Postma	n		
			🛆 Working	locally in Scratch P	ad. Swit	tch to a Workspace		
Scratch Pad	New Import	Overvie	9W	POST https://m	ıg-v-pba.	• + 000		
Collections	+ = 000	http:	s://mg-v-pba1/excl	hange/key				
oo APIs		POS	T ~ http	os://mg-v-pba1/ex	change/k	key		
Environments	s Contraction		Params Authorization Headers (7) Body Pre-request Script Te Query Params					
-		KEY				VALUE		
Mock Servers	You don't have any collections		Value					
An Monitors	Collections let you group related requests, making them easier to access and run. Create Collection							
History		Body Cookies Headers (4) Test Results						
		Pret	tty Raw P	review Visual	ize	⊊ ∨ nosl		
		1 2 3 4 5	f "error_ty "message" "response	ype": 1000, ": "invalid cli e_type": "Error	ent",			

Meldet sich der ServiceOutside mit der Antwort error_type: 1000 "invalid client", heißt es, dass die Verbindung zum ServiceOutside erfolgreich war und es kann nun mit der Installation und Einrichtung vom ServiceInside begonnen werden. 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 diese bitte zuerst, bevor Sie mit der Konfiguration vom ServiceInside fortsetzen.





 Als nächstes führen Sie bitte die Installationsdatei "dotnet-hosting-6.0.8-win.exe" im Verzeichnis "NET 6" aus und installieren Sie das .NET Framework 6.



- 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 "Inside" 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.

115) Internet Information Services (IIS)	Manager				
← → 🙆 ► MG-V-PBA2 ►	Sites 🕨		Add Website	?)	×
File View Help			Site name: Application pool:		
Connections	Sites		Inside DefaultAppPool Select		
S- 🗄 🔼 😣			Content Directory		
Start Page	Filter:	- 🛒 Go	Physical nath:		
Application Page	Name	ID	C:\inetpub\wwwroot		1
Sites			Pass-through authentication		
			Connect as Test Settings		
			Binding		
			Type: IP address: Port:		
			https V All Unassigned V 443		
			Host name:		
			mg-v-pba2		
			Require Server Name Indication		
			Disable HTTP/2		
			Disable OCSP Stapling		
			SL certificate:		
			MG-V-DC0002.labor-stein.de View		
			Start Website immediately		
			ок	Cancel	
	Eastures View PC	Content View			

Wichtig: Es muss ein gültiges Zertifikat verwendet werden.

5. Für die Verschlüsselung der Befunde und die Steuerung des LIS, verwendet den ServiceInside einen Hintergrundprozess, welcher auf Dauer aktiv bleiben muss. Um die Unterbrechung dieses Prozesses zu vermeiden, passen Sie bitte den "**Start** **Mode**", die **"Idle Time-Out**", **"Preload Enabled**" und den **"autoStart**" in IIS-Einstellungen entsprechend an:

Start Mode: AlwaysRunning. Idle Time-out: 0 Preload Enabled: True autoStart: True



File View Help		Advanced Settings		? ×		
Connections Connections Start Page MG-V-PBA2 (MG-V-PBA2\PBA) Application Pools Connection MG-V-PBA2 (MG-V-PBA2\PBA) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2\PBA)) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2\PBA)) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2\PBA)) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2\PBA)) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2)) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2)) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2)) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2)) MG-V-PBA2 (MG-V-PBA2 (MG-V-PBA2)) MG-V-PBA2 (MG-V-PBA2) MG-V-PBA2 (MG-V-PBA2) (MG-V-PBA2)) MG-V-PBA2 (MG-V-PBA2) (MG-V-PBA2) (MG-V-PBA2)) MG-V-PBA2 (MG-V-PBA2) (MG-V-PA2) (MG-V-PBA2) (MG-V-PA2) (MG-V	Filter: IIS Authentic MIME Types Manageme Egg	V (General) Application Pool Bindings ID Name Physical Path Physical Path Credentials Physical Path Credentials Le Preload Enabled Behavior Enabled Protocols HSTS Limits	DefaultAppPool https:*:443:mg-v-pba2 1 Inside C:\inetpub\wwwroot soon ClearText True 3 https		Logging	Actions Explore Edit Permissions Edit Site Bindings Basic Settings View Applications View Virtual Directories Manage Website C Restart Start Start Storp Browse Website Browse Website Browse mg-v-pba2 on *:443 (https)

Im "Configuration Editor" muss noch den "autoStart" aktiviert werden:



nternet Information Services (IIS) Manager

→ MG-V-PBA2 →					
: View Help					
nections Image Start Page Image Image	Sec	Configuration	Editor t/applicationPools +	4	
Application Pools	~	Deepest Path: MACHINE/V	VEBROOT/APPHOST		
Sites		(Collection)	(Count:	=1)	5 .
	>	applicationPoolDefaults			
	>	applicationPoolsControl			

Ite	ms:										
	name	queueLength	autoStart	enable32BitAppOnWin64	managedRuntimeVersion	managedRuntimeLoader	enableConf	igurationOverride	managedPipelineMode	CLRConfigFile	passAnonymo
	DefaultAppPool	1000	True	False	v4.0	webengine4.dll	True		Integrated		True
<											
Pr	operties:										
2	annlicationPoolSig	4				S-1-5-82-3006700770	424185610-1	745488364-794895	919-4004696415		
Г	autoStart					True		6			
h	CERCONTIGFILE							-			
>	cpu										
	enable32BitAppOr	nWin64				False					
	enableConfigurati	onOverride				True					
	environmentVarial	bles				(Count=0)					
>	failure										
	managedPipeline	Vlode				Integrated					
	managedRuntime	Loader				webengine4.dll					
	managedRuntime	Version				v4.0					
	name					PofaultAppPool					
	passAnonymousT	oken				True					
~	processModel										
	identityType					ApplicationPoolIden	tity				
	idleTimeout					00:00:00	7				
	idleTimeoutA	tion				Terminate					
	loadUserProfil	e				False					
	logEventOnPro	ocessModel				IdleTimeout					
	logonType					LogonBatch					
	manualGroup	Membership				False					
	maxProcesses					1					
	password										
	pingingEnable	d				True					
	pingInterval					00:00:30					
	pingResponse	Time				00:01:30					
	setProfileEnvir	onment				True					

6. Öffnen Sie die "appsettings.json" Datei im Verzeichnis "C:\inetpub\wwwroot", um den ServiceInside vollständig zu konfigurieren.

Th	is PC > Local Disk (C:) > inetpub > wwwroot			
	Name	Date modified	Туре	Size
	appsettings.json	8/11/2022 4:46 PM	JSON File	
۴	AspNetCoreRateLimit.dll	3/12/2022 12:41 PM	Application extens	
P.	aspnetcorev2_inprocess.dll	2/24/2022 9:50 AM	Application extens	
	Dounce/Castle Counte dll	2/10/2021 10:04 DM	Application extens	

 Tragen Sie in den Feldern "ServiceOutsideIP" und "ServiceOutsideURL" die IP und die URL vom ServiceOutside ein



8. Für die Datenbankverbindung tragen Sie bitte in der Konfigurationsdatei "appsettings.json" unter "ConnectionString" bei default "prod" und im prod ersetzen Sie die Daten durch die echten Daten von Ihrem MySQL Server.



Verschlüsselter ConnectionString



Bitte legen Sie in der Konfigurationsdatei "**appsettings.json**" die Pfade für die Verzeichnisse "**private**" und **"public**" fest. Das Verzeichnis "**private**" muss anschließend

für LIS/MIRTH/etc... freigegeben werden. In dieser Freigabe, sollen die Dateien vom LIS/MIRTH/etc... zur Steuerung der Backendservices gelesen und geschrieben werden. (S. Dokumentation über die LIS-Anbindung). Wichtig: Bitte nur das Verzeichnis "**private**" freigeben. Das Verzeichnis "**public**" wird vom ServiceInside für interne Zwecke verwendet.

"CleanUpDays": 30, "PrivateDirectory": "c:\\pba\\private", "PublicDirectory": <a>[c:\\pba\\public" "MaxWorkerThreads": 10, "ServiceOutsideIP": "172.21.16.98",

9. Starten Sie nun die neu angelegte Seite "Inside" im IIS Manager.



- 10. Zum Testen vom ServiceInside führen Sie bitte die Anwendung "Postman.exe" im Verzeichnis "Postman" aus. Anschließend führen Sie bitte in der Postman eine HTTPS POST-Abfrage mit der URL Hostname/exchange/key aus.
 - z.B: https://mg-v-pba2/exchange/key

🧭 Postman			
File Edit Vi	ew Help		
Home \	Norkspaces V Reports	Explore	Q Search Postman
			公 Working locally in Scratch Pad. Switch to a Workspace
Scratch Pad		New Import	Overview POST https://mg-v-pba • + ••••
Collections	+ =	000	https://mg-v-pba2/exchange/key
00 APIs	(°)	_	POST ~ https://mg-v-pba2/exchange/key
Environments			Params Authorization Headers (7) Body Pre-request Sc Query Params
	00		KEY VALUE
Mock Servers	You don't have any co	llections	Key Value
An Monitors	Collections let you group rela making them easier to acco	ated requests, ess and run.	
9	Create Collectio	n	
History			Body Cookies Headers (4) Test Results
			Pretty Raw Preview Visualize JSON ~ =
			<pre>1 2 "error_type": 1000, 3 "message": "invalid client", 4 "response_type": "Error" 5 2</pre>

Sollte der Webserver eine Antwort mit dem error_type: 1000 "invalid client" zurück liefern, so wurde der ServiceInside erfolgreich eingerichtet. Sollte der ServiceInside bei der Abfrage nicht korrekt reagieren, aktivieren Sie bitte in der Konfigurationsdatei "**appsettings.json**" den **DEBUG** Log und legen Sie einen Pfad für die Protokollierung der Fehler fest. Der ServiceInside protokolliert nun alle Abfragen mit den Fehlern in der Datei.

"Log": {
 "Type": "DEBUG",
 "Path": "c:\\tmp\\inside",
 "Control control con"

Zur weiteren Recherche von Problemen kann auch in der

"C:\inetpub\wwwroot\web.config" Datei die Protokollierung der Console-Ausgabe aktiviert werden.

Verschlüsseltes SmtpPassword

"SmtpPort": 25, "SmtpSSL": false, "SmtpUsername": "SmtpUser", "SmtpPassword": "yd/KLV70/pXzyHaveZM3b01CfcVkLFlkDVHXYU0GrQv6B+w=",



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

Einstellungen der erneuten Anfragen an LIS

Sollte das LIS bei der initialen Anfrage (.log – SUBSCRIBE) keinen Auftrag in seinen Stammdaten finden, kann der ServiceInside so konfiguriert werden, dass er nach bestimmter Zeit dem LIS erneut die Anfrage sendet.

"MaxTryNotFoundResults": 2, // Number of tries to check not found results "CheckIntervalNotFoundResultsInMinutes": 1440, // Time interval in minutes to check not found results again "ServiceOutsideIP": "::1", // IP of service outside to whitelist for communication (trusted header)

Der Parameter MaxTryNotFoundResults legt die Anzahl der Versuche von nicht gefundenen Befunden fest.

Der Parameter CheckIntervalNotFoundResultsInMinutes legt das Zeitintervall fest, in dem der ServiceInside die eneuten Anfrage an LIS bzgl. nicht gefundenen Befunde senden soll.

Ist der Parameter MaxTryNotFoundResults mit dem Wert 2 und der Parameter CheckIntervalNotFoundResultsInMinutes mit dem Wert 1440(24 Std.) parametrisiert, so sendet der ServiceInside insgesamt zwei Mal innerhalt 48 Std. (je nach 24 Std.) dem LIS eine erneute Anfrage (.log – SUBSCRIBE)