

Vorbereitung Installation «gemdat bau» für HTML5- Installationen

Rollenverzeichnis

Rolle	Mitarbeiter
Dokumentenverantwortlicher	Gemdat
Reviewzirkel	Gemdat
Zielgruppe	IT Gemdat

Änderungsverzeichnis

Datum	Änderungen	Version	Person
02.10.2026	Kap. 7 Process (Container/Helm Chart, Registry harbor.gemdat.ch) und Kap. 8 E-Mail Benachrichtigung (SMTP/Listmonk) ergänzt	1.4	Fabian Graf
05.08.2026	Azure Konfiguration für Dokumentenbearbeitung (WebDav) entfernt (Kap. 5.1.1/5.2.1)	1.3	Marco Sutter
31.03.2026		1.2	Nguyen Ly
31.07.2025	Ergänzung Kap 7.2 bzgl. Popup	1.1	Tanja Muñoz
28.03.2025	Neuerstellung Dokument für HTML5	1.0	Tanja Muñoz

Zweck des Dokuments

Dieses Dokument beschreibt die Vorbereitungsarbeiten für die Installation von «gemdat bau» in der Cloud. **Die HTML5-Installation für die Version 7.6 ist nur für den Einsatz in der Gemdat-Cloud und OnPrem freigegeben.**

Inhalt

1	Allgemeines	4
1.1	Ziele	4
1.2	Informationen	4
1.3	Anhang	4
2	Installation Webserver-Rolle	5
2.1	Beschreibung	5
2.2	Installation .NET	5
2.3	IIS Rollen	6
2.4	Betrieb über HTTPS	7
3	Einrichtung SQL-Server	7
3.1	Beschreibung	7
3.2	Kompatibilität zu Gemdat/5	8
4	Einrichten ActiveDirectory	9
4.1	Beschreibung	9
4.2	Anmeldeberechtigungen für den Dienstbenutzer vergeben	9
4.3	E-Mail-Feld bei Benutzern mit «gemdat archiv» oder «gemdat sign»	9
5	Konfiguration der Autorisierungs-Instanzen	10
5.1	Konfiguration «Microsoft Entra ID»	10
5.1.1	Konfiguration Backend App Registration	10
5.1.2	Konfiguration Frontend- App	11
5.1.3	Einrichtung der Sicherheitsgruppen und Benutzer	12
5.2	Konfiguration «gemdat bau»	13
5.2.1	Microsoft Entra ID	13
6	DNS Konfiguration	13
6.1	Beschreibung	13
7	Vorbereitungen Process	15
7.1	Beschreibung	15
7.2	Voraussetzungen Container-Plattform	15
7.3	Netzwerk, DNS und Zertifikat	15

7.4	Datenbank	16
7.5	Microsoft Entra ID	16
7.6	Zugriff auf die Container-Registry	17
7.7	Konfiguration (values-Dateien) & Secrets	17
8	Vorbereitung E-Mail Benachrichtigung (Abonnierte Ereignisse)	17
8.1	Beschreibung	17
8.2	Allgemeine Voraussetzungen	17
8.3	Versand über Listmonk	18
9	Anhang A: Checkliste	19
10	Anhang B: Infoblatt Entra ID	20
11	Anhang D: Update von früheren Versionen	22
12	Anhang E: Hinweis zum Setup ausführen	22

1 Allgemeines

1.1 Ziele

Der Administrator muss die Infrastruktur so weit vorbereiten, dass eine Installation von «gemdat bau» durch Gemdat AG ohne Neustart des Systems vorgenommen werden kann.

1.2 Informationen

Datenbankserver, Applikationsserver (Webserver) und Dateiablage können zusammen auf einem oder auch getrennt auf mehreren Servern betrieben werden.

Dieses Dokument beschreibt die minimal notwendigen Anforderungen an Datenbank und Webserver. Optional können weitere Features installiert werden.

1.3 Anhang

- Checkliste Vorbereitung
- Infoblatt (Server Informationen)
- Update von früheren Versionen

2 Installation Webserver-Rolle

2.1 Beschreibung

Auf dem Applikationsserver muss die Webserver-Rolle IIS installiert werden. Die für «gemdat bau» erforderlichen Rollendienste und Features sind in diesem Abschnitt beschrieben. Falls die IIS Rolle bereits installiert ist, muss kontrolliert werden, ob alle erforderlichen Features installiert sind.

2.2 Installation .NET

.NET muss gemäss dem Dokument «Technische Voraussetzungen» installiert sein.

2.3 IIS Rollen

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-WindowsFeature -Name Web*, Net* | where Installed

Display Name                                         Name                                Install State
-----
[X] Web Server (IIS)                                Web-Server                         Installed
[X] Web Server                                       Web-WebServer                     Installed
[X] Common HTTP Features                           Web-Common-Http                   Installed
[X] Default Document                               Web-Default-Doc                   Installed
[X] Directory Browsing                             Web-Dir-Browsing                  Installed
[X] HTTP Errors                                     Web-Http-Errors                   Installed
[X] Static Content                                 Web-Static-Content                Installed
[X] HTTP Redirection                               Web-Http-Redirect                 Installed
[X] Health and Diagnostics                         Web-Health                        Installed
[X] HTTP Logging                                   Web-Http-Logging                  Installed
[X] Logging Tools                                  Web-Log-Libraries                 Installed
[X] Request Monitor                                Web-Request-Monitor               Installed
[X] Security                                         Web-Security                      Installed
[X] Request Filtering                              Web-Filtering                     Installed
[X] Application Development                         Web-App-Dev                       Installed
[X] .NET Extensibility 4.8                         Web-Net-Ext45                     Installed
[X] Application Initialization                     Web-AppInit                       Installed
[X] ASP                                              Web-ASP                           Installed
[X] ASP.NET 4.8                                    Web-Asp-Net45                     Installed
[X] CGI                                              Web-CGI                           Installed
[X] ISAPI Extensions                              Web-ISAPI-Ext                     Installed
[X] ISAPI Filters                                  Web-ISAPI-Filter                  Installed
[X] WebSocket Protocol                             Web-WebSockets                   Installed
[X] Management Tools                               Web-Mgmt-Tools                    Installed
[X] IIS Management Console                         Web-Mgmt-Console                  Installed
[X] .NET Framework 4.8 Features                    NET-Framework-45-Fea...           Installed
[X] .NET Framework 4.8                             NET-Framework-45-Core             Installed
[X] ASP.NET 4.8                                    NET-Framework-45-ASPNET           Installed
[X] WCF Services                                    NET-WCF-Services45                Installed
[X] HTTP Activation                                NET-WCF-HTTP-Activat...           Installed
[X] Message Queuing (MSMQ) Activation               NET-WCF-MSMQ-Activat...           Installed
[X] Named Pipe Activation                           NET-WCF-Pipe-Activat...           Installed
[X] TCP Activation                                  NET-WCF-TCP-Activati...           Installed
[X] TCP Port Sharing                               NET-WCF-TCP-PortShar...           Installed

PS C:\WINDOWS\system32>
```

Wichtig: Nachfolgende Hinweise beachten!

Import-Module ServerManager

Get-WindowsFeature -Name web*, Net* | where Installed

Einstellungen:

- IIS Feature: Urlrewrite 2.1 muss installiert sein
- IIS Performance Feature «dynamic content compression» muss deaktiviert oder deinstalliert sein
- IIS Performance Feature «static content compression» muss deaktiviert oder deinstalliert sein

Hinweis:

Name des Applikationsservers auf Infoblatt vermerken!

2.4 Betrieb über HTTPS

Damit «gemdat bau» über HTTPS betrieben werden kann, ist der Kunde für ein passendes Zertifikat verantwortlich. Dieses muss auf dem Applikationsserver installiert sein.

Hinweis:

Weitere Infos unter Kapitel 6 DNS Konfiguration

3 Einrichtung SQL-Server

3.1 Beschreibung

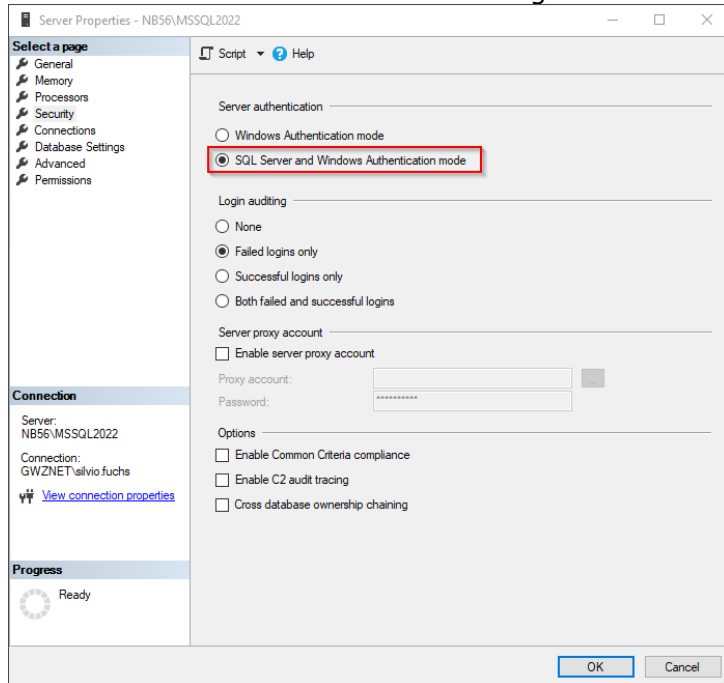
Als Datenbank-Server wird Microsoft SQL in englischer Standardsprache vorausgesetzt. Gemdat empfiehlt die Installation einer Test- und Produktiv-Datenbank. Die beiden Datenbanken können wahlweise auf unterschiedlichen Instanzen oder Servern betrieben werden.

Hinweis:

Datenbank-Server Host Name, SQL Server Instanz Name und Datenbank Name im Infoblatt ergänzen.

3.2 Kompatibilität zu Gemdat/5

Falls «GemDat/5» und «gemdat bau» parallel betrieben werden, wird «SQL Server and Windows Authentication Mode» benötigt.



Für «gemdat bau» allein genügt «Windows Authentication Mode».

4 Einrichten ActiveDirectory

4.1 Beschreibung

Um die JobEngine und den Anwendungspool von «gemdat bau» auszuführen, wird ein Domänen-Benutzer (Dienstbenutzer) benötigt. Dieser Benutzer wird später als Dienstbenutzer für den GemDatJobEngine-Dienst (Windows Service) und den IIS-Anwendungspool benötigt.

Hinweis:

Benutzernamen auf Infoblatt im Anhang vermerken!

4.2 Anmeldeberechtigungen für den Dienstbenutzer vergeben

Der «gemdat bau»-Dienstbenutzer benötigt auf dem Applikationsserver Anmeldeberechtigung als Dienst und Stapelverarbeitungsauftrag.

4.3 E-Mail-Feld bei Benutzern mit «gemdat archiv» oder «gemdat sign»

Damit sich ein «gemdat archiv» Benutzer auch erfolgreich bei «gemdat archiv» oder «gemdat sign» authentifizieren kann muss im entsprechenden Verzeichnisdienst (z.B. Active Directory oder Entra-ID) auf dem Benutzerobjekt das E-Mail-Feld abgefüllt sein. Falls der/die Benutzer/in keine E-Mail besitzt kann auch eine nicht funktionierende oder erfundene E-Mail-Adresse verwendet werden.

5 Konfiguration der Autorisierungs-Instanzen

«gemdat bau» unterstützt für die HTML5 Installationen mit 7.3 «Microsoft Entra ID» als Benutzer Autorisierungs- Instanzen. «Microsoft Active Directory» ist hingegen nicht mehr unterstützt. Für die Verwendung von EntraID ist die Einrichtung der Installation auf HTTPS unter Punkt 2.4 zwingend.

Die Benutzer Authentifizierung erfolgt für die WebClients im Frontend nach dem «OAuth 2.0 authorization code grant» Flow.

5.1 Konfiguration «Microsoft Entra ID»

Für «gemdat bau» müssen in Microsoft Entra ID zwei App Registrations vorgenommen werden, je eine Registration für die Frontend- und Backend- App:

- gemdat bau [name]-frontend
- gemdat bau [name]-backend

(Die Namensgebung muss nicht zwingend dem vorgeschlagenen Namensschema folgen, es gibt diesbezüglich keine Restriktionen)

5.1.1 Konfiguration Backend App Registration

Tab «Tokenkonfiguration»

Es sind folgende optionalen Ansprüche zu konfigurieren:

Anspruch ↑↓	Beschreibung	Token typ ↑↓	Optionale Einstellungen
family_name	Gibt den Nachnamen oder Familiennamen des Benutzers gemäß Definition im Benutzerobjekt an.	ID	-
family_name	Gibt den Nachnamen oder Familiennamen des Benutzers gemäß Definition im Benutzerobjekt an.	Zugriff	-
given_name	Gibt den Vornamen des Benutzers gemäß Festlegung im Benutzerobjekt an.	ID	-
given_name	Gibt den Vornamen des Benutzers gemäß Festlegung im Benutzerobjekt an.	Zugriff	-
groups	Optionale Formatierung für Gruppenansprüche	ID, Zugriff, SAML	Ja
upn	Ein Bezeichner für den Benutzer, der mit dem username_hint-Parameter verwendet werden kann. Es handelt sich nicht um einen dauerhaften...	ID	Ja
upn	Ein Bezeichner für den Benutzer, der mit dem username_hint-Parameter verwendet werden kann. Es handelt sich nicht um einen dauerhaften...	Zugriff	Ja

Beim UPN Access Token müssen die Optionen «Externally authenticated» und «Replace hash marks» aktiviert werden.

Tab «Eine API verfügbar machen»

Ein neuer Bereich «Bau.All» muss gemäss folgendem Schema zugefügt werden:

- api://[clientId]/Bau.All

wobei [clientId] der Application (client) ID der Backend App Registration entsprechen soll.

Beispiel:

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. [Go to App roles.](#)

+ Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
api://.../Bau.All	Admins only	Bau Alle Berechtigungen		Enabled

Hinweis:

Client ID und Bereich (Audience) auf Infoblatt im Anhang vermerken!

5.1.2 Konfiguration Frontend- App

Tab «Authentifizierung»

Hier müssen die Redirect URLs für die «Single-Page-Webanwendung» für den «OAuth 2.0 authorization code grant flow» erfasst werden.

Konkret müssen 4 URLs registriert werden: Html5 Bau und Admin mit und ohne redirect. Dabei ist zu beachten, dass die URLs exakt der Installation vom «gemdat bau» entsprechen müssen (Registrierte Domain, Webseite im IIS, Relativer Pfad der Webanwendung):

- `https://[domain]/[site]/[page]`

Beispielkonfiguration:

Client	Client Typ	Beispiel Redirect Url
Admin Client	Html	<code>https://gemdat.contoso.com/bau/bau-client-admin</code>
Admin Client	Html	<code>https://gemdat.contoso.com/bau/bau-client-admin/redirect</code>
Bau Client	Html	<code>https://gemdat.contoso.com/bau/bau-client</code>
Bau Client	Html	<code>https://gemdat.contoso.com/bau/bau-client/redirect</code>

Keine impliziten Genehmigungen:

Wählen Sie die Token aus, die vom Autorisierungsendpunkt ausgegeben werden sollen:

- ☐ Zugriffstoken (werden für implizite Flows verwendet)
- ☐ ID-Token (werden für implizite und Hybridflows verwendet)

Tab «Tokenkonfiguration»

Es sind folgende optionalen Ansprüche (Claims) hinzuzufügen.

Anspruch ↑	Beschreibung	Token typ ↑↓	Optionale Einstellungen
family_name	Gibt den Nachnamen oder Familiennamen des Benutzers gemäß Definition im Benutzerobjekt an.	ID	-
given_name	Gibt den Vornamen des Benutzers gemäß Festlegung im Benutzerobjekt an.	ID	-
upn	Ein Bezeichner für den Benutzer, der mit dem username_hint-Parameter verwendet werden kann. Es handelt sich nicht um einen dauerhaften...	ID	Ja

Beim UPN ID Token müssen die Optionen «Externally authenticated» und «Replace hash marks» aktiviert werden.

Tab «API-Berechtigungen»

Um die zuvor im Backend zur Verfügung gestellte API hinzuzufügen, kann über den Button «Berechtigung hinzufügen» zunächst ein Dialog geöffnet werden, wo im Tab «Von meiner Organisation verwendete API's» die API der Backend App Registration ausgewählt werden muss.

Es wird die Berechtigungen für Bau.All und Process.All (siehe Kap. 7.5) benötigt.

Nach der korrekten Zuweisung sieht das beispielsweise so aus:

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission		✓ Grant admin consent for Gemdat AG Dev		
API / Permissions name	Type	Description	Admin consent req...	Status
▼ app-process-dev-local-backend (1) ***				
Process.All	Delegated	Process.All	Yes	✓ Granted for Gemdat AG ... ***
▼ gemdat bau ent dev-backend (1) ***				
Bau.All	Delegated	Bau Alle Berechtigungen	Yes	✓ Granted for Gemdat AG ... ***

Administratoreinwilligung muss gewährt werden.

5.1.3 Einrichtung der Sicherheitsgruppen und Benutzer

Im gleichen Tenant, in dem die App- Registrationen vorgenommen worden sind, sind die gewünschten Sicherheitsgruppen anzulegen. Zudem müssen die Benutzer für «gemdat bau» angelegt und den entsprechenden Sicherheitsgruppen zugewiesen werden. Typische Sicherheitsgruppen sind:

Folgende Benutzer und Sicherheitsgruppen sind empfohlen:

Bezeichnung	AD Typ	Beschreibung
Gemdat_TestUser	Benutzer	Testbenutzer für den Funktionstest nach der Installation. (Stellt einen Mitarbeiter dar, welcher mit «gemdat bau» arbeitet)
Gemdat_Administratoren	Gruppe	Gruppe für die Administration von «gemdat bau» (zwingend erforderlich)
Gemdat_Bauverwaltung	Gruppe	Sicherheitsgruppe für «gemdat bau» (Standard-) Anwender
Gemdat_Lesend	Gruppe	Sicherheitsgruppe für «gemdat bau» Anwender mit Leseberechtigung

Die UUID's (Universally Unique Identifier) dieser Entra ID Sicherheitsgruppen müssen in der Bau Anwendung den Bau Sicherheitsgruppen zugewiesen werden.

Hinweis:

Die Administratoren Sicherheitsgruppe ist zwingend erforderlich. Die UUID der Administratoren Sicherheitsgruppe auf Infoblatt im Anhang vermerken!

5.2 Konfiguration «gemdat bau»

5.2.1 Microsoft Entra ID

Benutzer Authentifizierung Web Client

Parameter	Wert
TenantId	TenantId von Microsoft Entra Id
ClientId	ClientId der Frontend App-Registrierung
Authority	https://login.microsoftonline.com/{TenantId}/v2.0
Audience	api://{clientId Backend}
ValidIssuers	https://login.microsoftonline.com/{TenantId}/v2.0 , https://sts.windows.net/{TenantId}/

6 DNS Konfiguration

6.1 Beschreibung

«gemdat bau» bzw. «gemdat bau»-Test werden über definierte URLs aufgerufen. Hierzu muss für jede Anwendung ein entsprechender DNS Eintrag erstellt werden.

Beispiel: Produktiv
Aufruf: <https://gemdat.contoso.com/bau>
DNS Eintrag:

New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank):
gemdat

Fully qualified domain name (FQDN):
gemdat.contosso.com.

Fully qualified domain name (FQDN) for target host:
192.168.1.105 Browse...

☐ Delete this record when it becomes stale

Record time stamp:

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

OK Cancel

Hinweis:

Bei der Verwendung von HTTPS muss der DNS-Eintrag mit dem verwendeten Zertifikat übereinstimmen!

7 Vorbereitungen Process

7.1 Beschreibung

Ab Version 7.6.0 wird ein Teil der Applikation («Process» / GEVER) als Linux-Container betrieben. Gemdat AG stellt dafür die Container-Images in der Registry harbor.gemdat.ch sowie ein Helm Chart (gemdat-process-apphost) bereit. «Process» besteht aus drei Komponenten, die je als eigener Pod laufen:

Komponente	Pfad (Ingress)	Beschreibung
process-webhost	/api	Backend (API), Konfiguration, Datenbankzugriff und E-Mail-Versand
app-process	/process	Frontend «Process»
app-process-execution	/process-execution	Frontend «Process Execution» (Ausführung)

7.2 Voraussetzungen Container-Plattform

Die Container-Plattform (Kubernetes-Version, Ressourcen pro Pod) muss den Anforderungen gemäss Dokument «Technische Voraussetzungen» entsprechen. Zusätzlich gilt:

- Helm (Version 3 oder höher) und kubectl mit Zugriff auf den Cluster sind auf dem Administrationsrechner installiert
- Eigener Namespace für «Process» ist erstellt (Beispiel: gemdat-process)
- Ingress-Controller ist installiert (Standard im Helm Chart: nginx). Alternativ wird Gateway API (HTTPRoute) mit einem bestehenden Gateway unterstützt
- Die Cluster-Richtlinien erlauben Pods mit Non-Root-Benutzer, schreibgeschütztem Root-Dateisystem und Seccomp-Profil «RuntimeDefault» (kompatibel mit Pod Security Standard «restricted»)

7.3 Netzwerk, DNS und Zertifikat

- DNS-Eintrag für den Process-Host ist erstellt, z.B. process.contoso.com (siehe Kapitel 6 DNS Konfiguration)
- Gültiges TLS-Zertifikat für den Process-Host ist als Kubernetes-Secret (Typ kubernetes.io/tls) im Namespace hinterlegt
- Die Nodes erreichen die Registry harbor.gemdat.ch über HTTPS (Port 443)
- Die Pods erreichen den SQL-Server der Process-Datenbank (Standard Port 1433)
- Die Pods erreichen Microsoft Entra ID (login.microsoftonline.com) sowie die Listmonk-Instanz über HTTPS
- Der Applikationsserver «gemdat bau» und die Clients erreichen den Process-Host über HTTPS (Port 443) in beiden Richtungen.

7.4 Datenbank

Die Anforderungen an die zusätzliche Process-Datenbank sind im Dokument «Technische Voraussetzungen» beschrieben. Vorzubereiten ist:

- Datenbank für «Process» ist erstellt (Beispiel: Process_prod / Process_test)
- SQL-Server läuft im «SQL Server and Windows Authentication Mode» (vgl. Kapitel 3.2), da sich der Linux-Container mit einem SQL-Login anmeldet
- SQL-Login für «Process» ist erstellt und auf der Process-Datenbank berechtigt (z.B. db_owner)

7.5 Microsoft Entra ID

«Process» verwendet für die Anmeldung die Backend- und Frontend-App-Registration aus Kapitel 5.1. Zusätzlich müssen bei der Frontend-App-Registration unter «Single-Page-Webanwendung» die Redirect URLs der beiden Process-Frontends erfasst werden:

Client	Beispiel Redirect Url
Process	https://process.contoso.com/process/redirect
Process Execution	https://process.contoso.com/process-execution/redirect

Tab «Eine API verfügbar machen» für Process Backend

Ein neuer Bereich «Process.All» muss gemäss folgendem Schema zugefügt werden:

- api://[clientId]/Process.All

Beispiel:

Scopes defined by this API Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these. Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles. + Add a scope				
Scopes	Who can consent	Admin consent display n...	User consent di...	State
api://[redacted]/Process.All	Admins only	Process.All		Enabled

Tab «API-Berechtigungen» für Process Frontend

Es wird die Berechtigung Process.All benötigt.

Beispiel:

Configured permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent + Add a permission ✓ Grant admin consent for Gemdat AG Dev				
API / Permissions name	Type	Description	Admin consent requ...	Status
app-process-dev-backend (1)				
Process.All	Delegated	Process.All	Yes	✓ Granted for Gemdat AG ...

7.6 Zugriff auf die Container-Registry

Die Zugangsdaten für die Gemdat Registry können bei der Gemdat AG im Helpdesk bezogen werden.

Registry URL:

<https://harbor.gemdat.ch>

7.7 Konfiguration (values-Dateien) & Secrets

Die Konfiguration erfolgt über zwei umgebungsspezifische Dateien, welche die Standardwerte des Helm Charts überschreiben. Alle Werte mit «VALUE_TO_OVERRIDE» müssen gesetzt werden.

Wichtig:

Der bei der Erstinstallation generierte ENCRYPTION_KEY (Secret «process-webhost-keys») verschlüsselt Daten in der Process-Datenbank. Das Secret darf nicht gelöscht werden und ist zusammen mit der Datenbank zu sichern.

8 Vorbereitung E-Mail Benachrichtigung (Abonnierte Ereignisse)

8.1 Beschreibung

Mit der Funktion «Abonnierte Ereignisse» können Benutzer von «gemdat bau» Ereignisse abonnieren und werden bei deren Eintreten per E-Mail benachrichtigt. Der E-Mail-Versand erfolgt über [Listmonk](#).

8.2 Allgemeine Voraussetzungen

- Bei allen Benutzern, die Benachrichtigungen erhalten sollen, ist im Verzeichnisdienst (Entra ID) das E-Mail-Feld abgefüllt (vgl. Kapitel 4.3)
- Eine Absenderadresse ist definiert (Beispiel: gemdat-bau@contoso.com)

8.3 Versand über Listmonk

Listmonk übernimmt den Versand der Benachrichtigungen. Die Anbindung wird in der Konfiguration von «Process» hinterlegt (siehe Kapitel 7.7). Die Listmonk-Instanz selbst muss mit einem SMTP-Server konfiguriert sein. Folgende Angaben werden benötigt:

Parameter	Beschreibung
Listmonk-URL	Basis-URL der Listmonk-Instanz (HTTPS), values: processWebhost.config.email.listmonk.baseUrl
Benutzer	Listmonk-Benutzer mit den benötigten Berechtigungen, values: ...listmonk.username
Access Token	Token des Listmonk-Benutzers, secrets: LISTMONK_ACCESS_TOKEN
Absenderadresse	Absender der E-Mails, values: ...listmonk.fromEmail

- In Listmonk ist ein SMTP-Server hinterlegt und getestet (Einstellungen > SMTP)
- In Listmonk ist ein API-Benutzer mit Token erstellt
- Firewall: Die «Process»-Pods erreichen die Listmonk-URL über HTTPS (Port 443)

9 Anhang A: Checkliste

- ☐ Server
 - ☐ IIS Rolle mit zugehörigen Rollendiensten und Features installiert
 - ☐ SQL-Server mit gewünschten Features installiert
 - ☐ Datenbank ist erstellt
- ☐ Active Directory
 - ☐ Anmeldeberechtigung des Dienstbenutzers konfiguriert
- ☐ Entra ID Konfiguration
 - ☐ Sicherheitsgruppen erstellt
 - ☐ Testbenutzer erstellt
 - ☐ App Registrations erstellt
 - ☐ Token konfiguriert
 - ☐ Konfiguration WebDav erstellt
- ☐ DNS Konfiguration
 - ☐ DNS Einträge erstellt
- ☐ Clients
 - ☐ Zonenkonfiguration in den Internetoptionen erstellt

10 Anhang B: Infoblatt Entra ID

(Kopie an Gemdat AG)

Umgebung:

	Produktivsystem:	Testsystem:
Name:		

SQL-Server Infos:

	Produktivsystem:	Testsystem:
SQL-Server Host Name:		
SQL-Server Edition/Version:		
SQL-Instanz Name:		
SQL-Datenbank Name:		

Applikationsserver (IIS) Infos:

	Produktivsystem:	Testsystem:
Servername:		
Site-URL:		
IIS-Webseiten HTTP/HTTPS (Port):	(80/443).....	(80/443).....
HTTPS Zertifikat vorhanden?		

Active Directory

Benutzername Dienstbenutzer:	

Microsoft Entra ID:

Tenant ID:	
Client ID (frontend):	
Audience:	
Authority:	
Open ID Config:	
Valid Issuer:	
Sicherheitsgruppe Administratoren UUID:	
Benutzername Testuser (optional):	

Dokumentenablage für Schnittstellen und Vorlagen:

Filesystem Verzeichnis:

Vorlagen Verzeichnis:

Temporäres Dokumentenverzeichnis:

Dokumentenhandling WebDav (HTML5):

Redirect Uri:

Tenant ID (wenn abweichend):

Client ID (Backend):

Audience (wenn abweichend):

Authority (wenn abweichend):

Open ID Config (wenn abweichend):

Valid Issuer (muss V1 und V2 hinterlegt werden):

Prozessablauf (HTML5):

Basis URL:

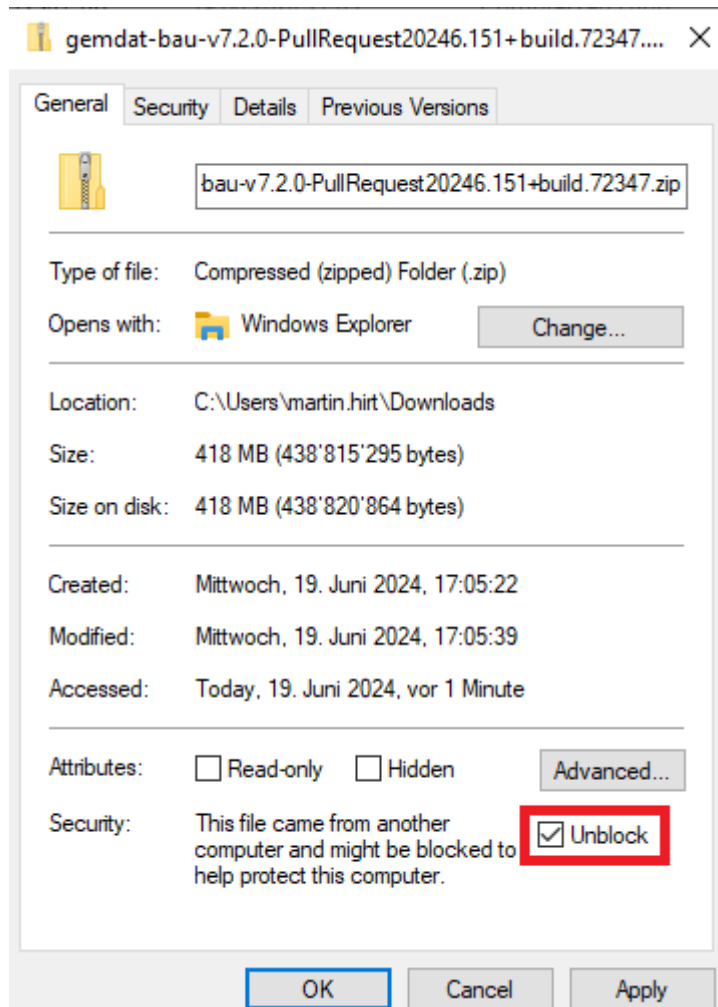
Kundeninstanz Identifikation:

11 Anhang D: Update von früheren Versionen

Mit der Version 7.6.0 steht «gemdat bau» als HTML5 Version für Neuinstallationen und Migrationen zur Verfügung. Bitte prüfen Sie vor dem Update alle Kapitel dieses Dokumentes!

12 Anhang E: Hinweis zum Setup ausführen

Die Setup-Dateien befinden sich in der Containerdatei (Beispiel: gemdat-bau-v7.2.0+30812.zip) und müssen zuerst entpackt werden. Beim Entpacken muss darauf geachtet werden, dass das Attribut 'Unblock' angekreuzt ist:



Das Setup kann nur noch im SilentMode mit Konfiguration über ein JSON File ausgeführt werden. Bitte wenden Sie sich dazu an den Gemdat Support.