



TIKOS

BUSINESS SOLUTIONS

AppServer

Installationshinweise

Allgemeiner Hinweis

Dieses Dokument gibt zahlreiche Anforderungen und Hinweise, um die Installation des AppServers erfolgreich durchzuführen.

Dieses Dokument ersetzt jedoch nicht die Mindestvoraussetzungen!

Reverse Proxy

Wenn ein Reverse Proxy eingesetzt werden soll, müssen folgenden Voraussetzungen erfüllt werden:

- Es wird entweder Apache oder Nginx empfohlen.
- Der Reverse Proxy sollte https für die Kommunikation mit dem AppServer verwenden.
- Es muss möglich sein, HTTP-Verbindungen mit dem AppServer aufzubauen und HTTPS-Requests an diesen zu senden.
- Es muss möglich sein, gRPC (http/2)-Verbindungen mit dem AppServer aufzubauen und gRPC-Requests an diesen zu senden.
- Sollte nginx eingesetzt werden, dürfen die Einstellungen „grpc_set_header Host“ und „proxy_set_header Host“ nicht verwendet werden, da diese beim IIS zu Problemen führen.

Konfigurationsbeispiele:

Apache:

Es müssen die Module mod_headers, mod_ssl, mod_http2, mod_proxy und mod_proxy_http2 aktiviert sein.

```
<VirtualHost *:443>
  # TODO: use correct external domain.
```



```
ServerName appserver.localhost  
Protocols h2 http/1.1
```

```
SSLEngine on  
SSLProxyEngine on  
# TODO: use correct certificate paths.  
SSLCertificateFile "/path/to/certificate.crt"  
SSLCertificateKeyFile "/path/to/certificate.key"
```

```
# TODO: use correct internal ip/domain and port of appserver.  
ProxyPass / h2://192.168.240.198:443/ keepalive=On upgrade=websocket  
ProxyPassReverse / h2://192.168.240.198:443/  
</VirtualHost>
```

Nginx:

Die Einstellungen `grpc_set_header Host` und `proxy_set_header Host` dürfen nicht gesetzt werden, da diese beim IIS Fehler erzeugen können (z.B. 400 BadRequest Fehler).

Bei der Verwendung von `grpc_ssl_verify` oder `proxy_ssl_verify` muss sichergestellt werden, dass die dazugehörigen Einstellungen (z.B: akzeptierte Zertifikate) korrekt gesetzt sind.

```
upstream appserver {
    # TODO: use correct internal ip/domain and port of appserver.
    server 192.168.240.198:443;
}

server {
    listen 443 ssl;
    http2 on;
    # TODO: use correct external domain.
    server_name appserver.localhost;

    # TODO: use correct certificate paths.
    ssl_certificate /path/to/certificate.crt;
    ssl_certificate_key /path/to/certificate.key;

    location / {
        grpc_connect_timeout 10s;
        grpc_read_timeout 300s;
        grpc_send_timeout 300s;

        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $http_connection;
        proxy_http_version 1.1;

        # Nginx does only allow http2 upstream connections for grpc requests.
        # But the AppServer does also provide for example a normal http api which would break if we
        use grpc_pass for everything.
        # Because of this we need to check the content type and decide what to do with the request.
        if ($http_content_type = "application/grpc") {
            grpc_pass grpcs://appserver;
        }

        proxy_pass https://appserver;
    }
}
```