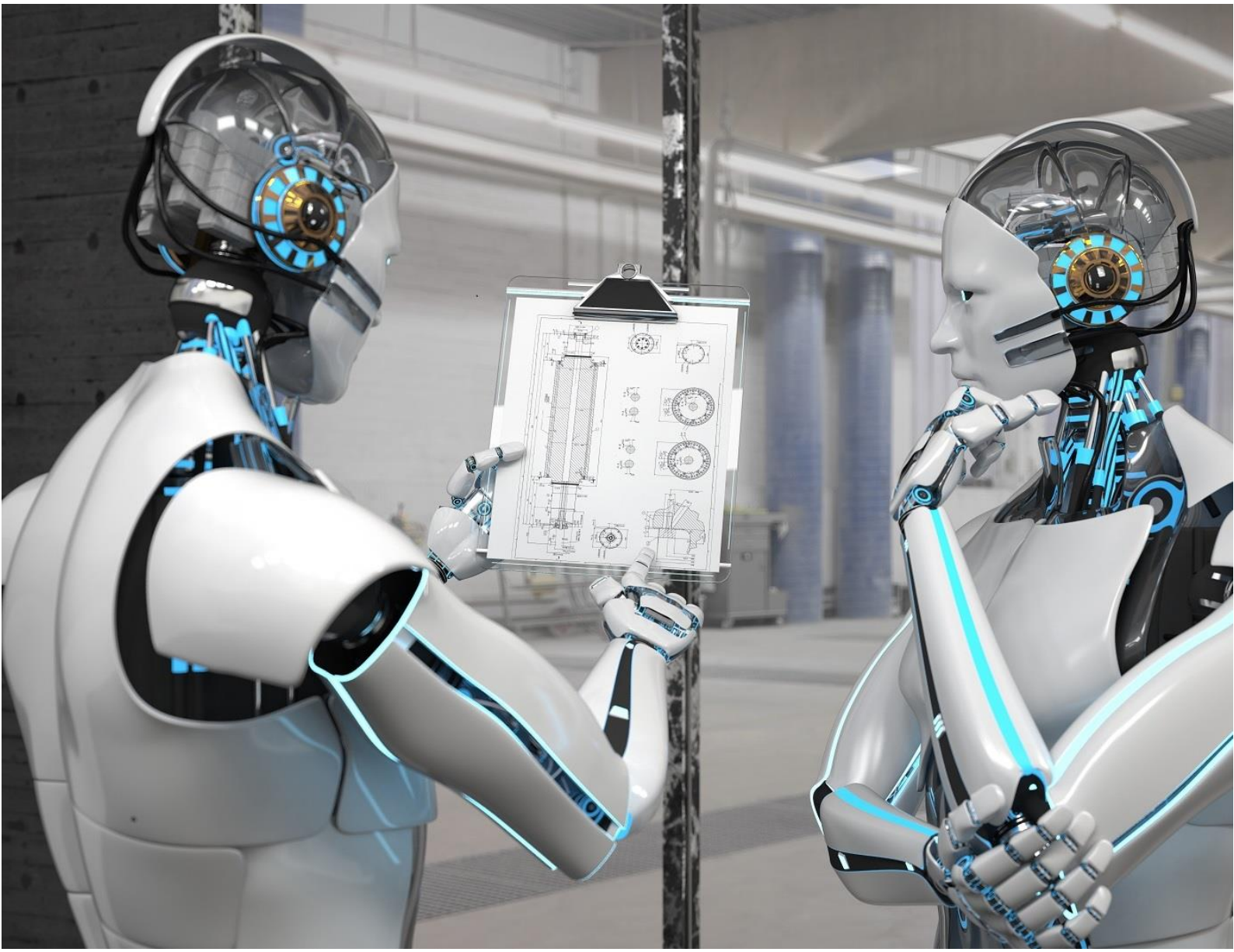
Symbio Cloud Operation



Inhalt

1 Symbio Cloud Operation

Aufbauend auf dem vorgehenden Kapitel werden die Cloud-spezifischen Einstellungen und Eigenschaften beschrieben. Es werden Informationen zum Cloud-Anbieter, zur Verschlüsselung und zum Datenschutz erläutert.

1.1 Allgemeine Informationen zum Cloud-Anbieter

Soweit Sie keine anderen vertraglichen Vereinbarungen getroffen haben, nutzt die Symbioworld GmbH für das Produkt Symbio Cloud die Plattform Services (PaaS) und die Infrastruktur Services (IaaS) von Microsoft Azure.

Weitere allgemeine Informationen zu Microsoft Azure:
https://azure.microsoft.com/de-de/

1.2 Wo befinden Sich Ihre Daten?

Soweit Sie keine anderen vertraglichen Vereinbarungen getroffen haben, werden Ihre Daten in den **europäischen** Rechenzentren der Firma Microsoft gespeichert. Alle Plattform- und Infrastruktur-Services speichern Ihre Daten ausschließlich auf europäischen Servern.

Auf Wunsch können Sie auch eine Private Cloud in Deutschland mit deutscher Datentreuhand beantragen. Sprechen Sie uns direkt an, falls Sie an diesem Service interessiert sind. Alle weiteren Informationen bzgl. Datenschutz beziehen sich auf die europäische Cloud.

Weitere Informationen von Microsoft:
https://www.microsoft.com/de-de/trustcenter/privacy/where-your-data-is-located

Für Kunden, die in stark regulierten Branchen oder in Ländern mit Datenschutzgesetzen tätig sind, ist es besonders wichtig, den geografischen Standort der Daten zu kennen, die Sie einem Microsoft Cloud Service anvertraut haben. Microsoft versteht auch, dass einige Kunden ihre Daten an einem speziellen geografischen Standort halten müssen, z. B. innerhalb der Europäischen Union (EU). Aus diesem Grund verfügt Microsoft über ein stetig wachsendes Netzwerk von Rechenzentren rund um den Globus und stellt sicher, dass die strengen Sicherheitsanforderungen von jedem einzelnen Rechenzentrum eingehalten werden.

- Kundendaten können innerhalb eines geografischen Gebiets repliziert werden, um die Lebensdauer der Daten für den Fall eines größeren Rechenzentrumnotfalls zu verbessern. In einigen Fällen werden sie außerhalb dieses Gebiets nicht repliziert.
- Microsoft hält Datenschutzgesetze im Hinblick auf die Übertragung von Kundendaten über Landesgrenzen hinaus ein. Beispiel:
    - Damit internationale Unternehmen von dem erforderlichen kontinuierlichen Informationsfluss profitieren (einschließlich der grenzüberschreitenden Übertragung personenbezogener Daten), bieten viele Microsoft Cloud Services für Unternehmen Kunden im Rahmen des Dienstleistungsumfangs EU-Standardvertragsklauseln mit zusätzlichen vertraglichen Garantien in Bezug auf die Übertragung personenbezogener Daten. Die Implementierung der EU-Standardvertragsklauseln wurde von Datenschutzbehörden der EU überprüft und ist im Einklang mit den strengen Datenschutzstandards, welche die internationale Übertragung von Daten durch Unternehmen regeln, die in den Mitgliedsstaaten der EU tätig sind.

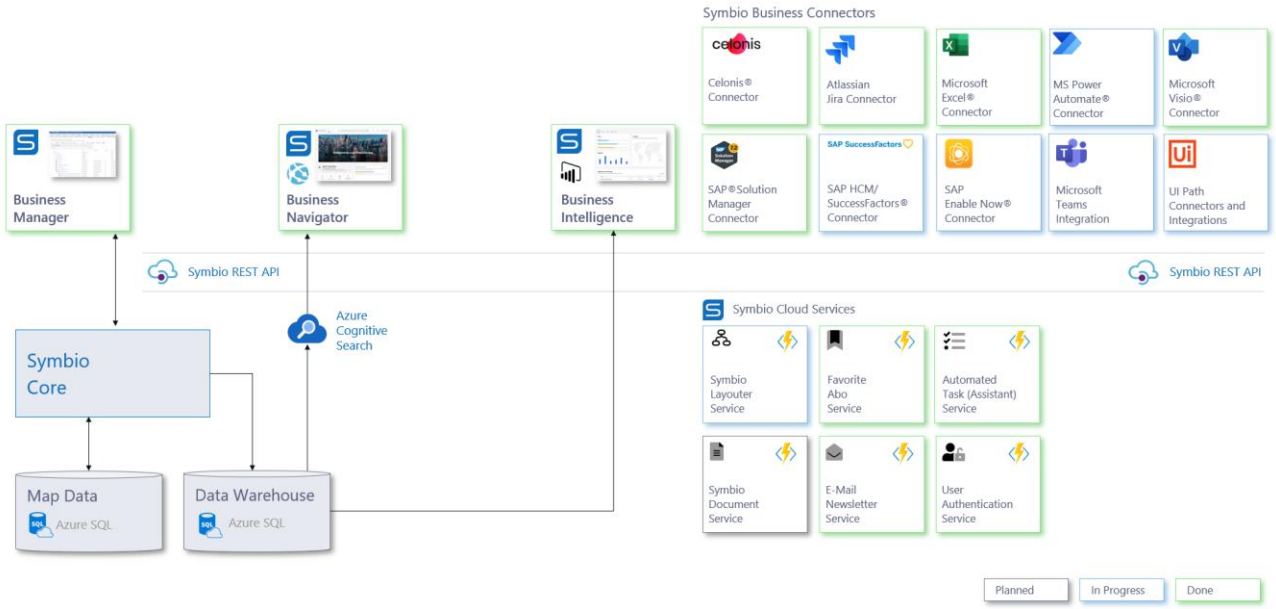
- Über unsere Verpflichtungen gemäß den Standardvertragsklauseln und anderen Musterverträgen hinaus, ist Microsoft vom EU-U.S. zertifiziert. Privacy Shield Framework, wie vom US Department of Commerce (US-amerikanisches Handelsministerium) dargelegt, im Hinblick auf die Erfassung, Verwendung und Vorhaltung von personenbezogenen Daten, die von der EU in die USA übertragen werden. Die Teilnahme von Microsoft am Privacy Shield gilt für alle personenbezogenen Daten, die dem Microsoft Privacy Statement unterliegen und aus der EU, dem Europäischen Wirtschaftsraum und der Schweiz stammen. Außerdem befolgt Microsoft die schweizerischen Datenschutzgesetze bezüglich der Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum und der Schweiz.
- Microsoft überträgt keine Daten an Dritte (auch nicht zu Speicherzwecken), die Sie Microsoft im Rahmen der Verwendung unserer Cloud Services für Unternehmen, die unter die Microsoft Online Services-Nutzungsbedingungen fallen, zur Verfügung stellen.

Microsoft kontrolliert oder beschränkt die Standorte nicht, aus denen Kunden oder ihre Endbenutzer auf ihre Daten zugreifen, unabhängig davon, wo die Kundendaten gespeichert sind.

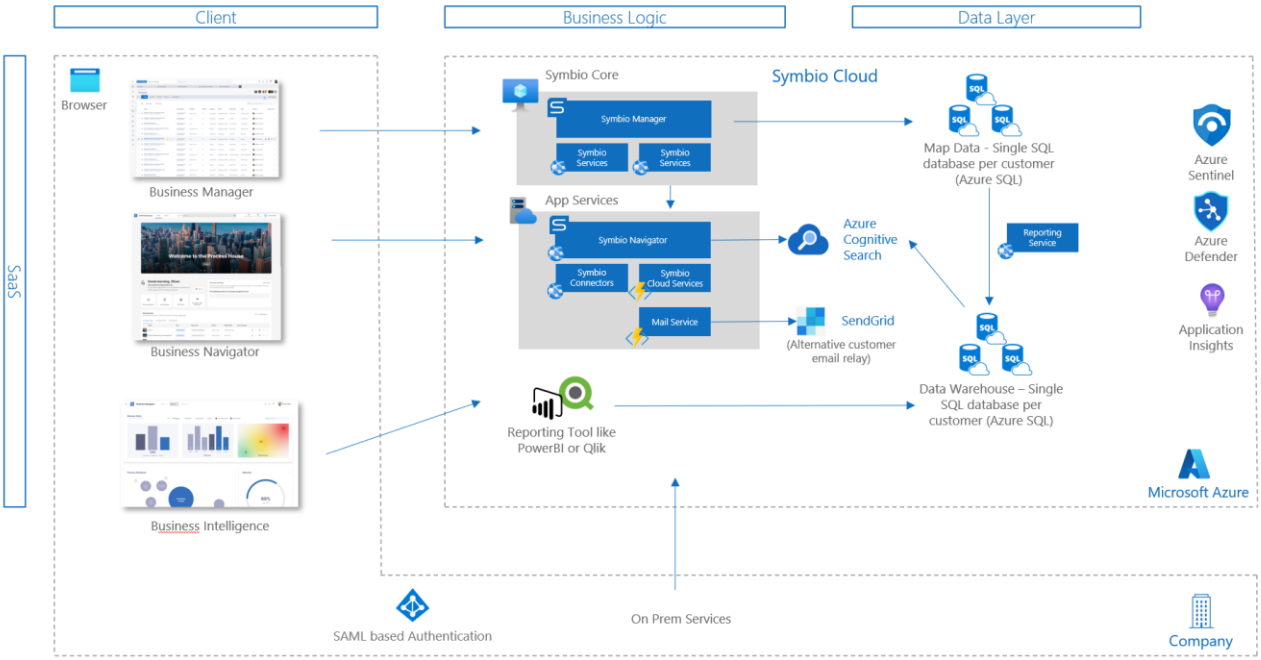
2 Cloud Übersicht

Überblick über die Symbio Cloud Architektur

2.1 Symbio Apps, Services and Connectors

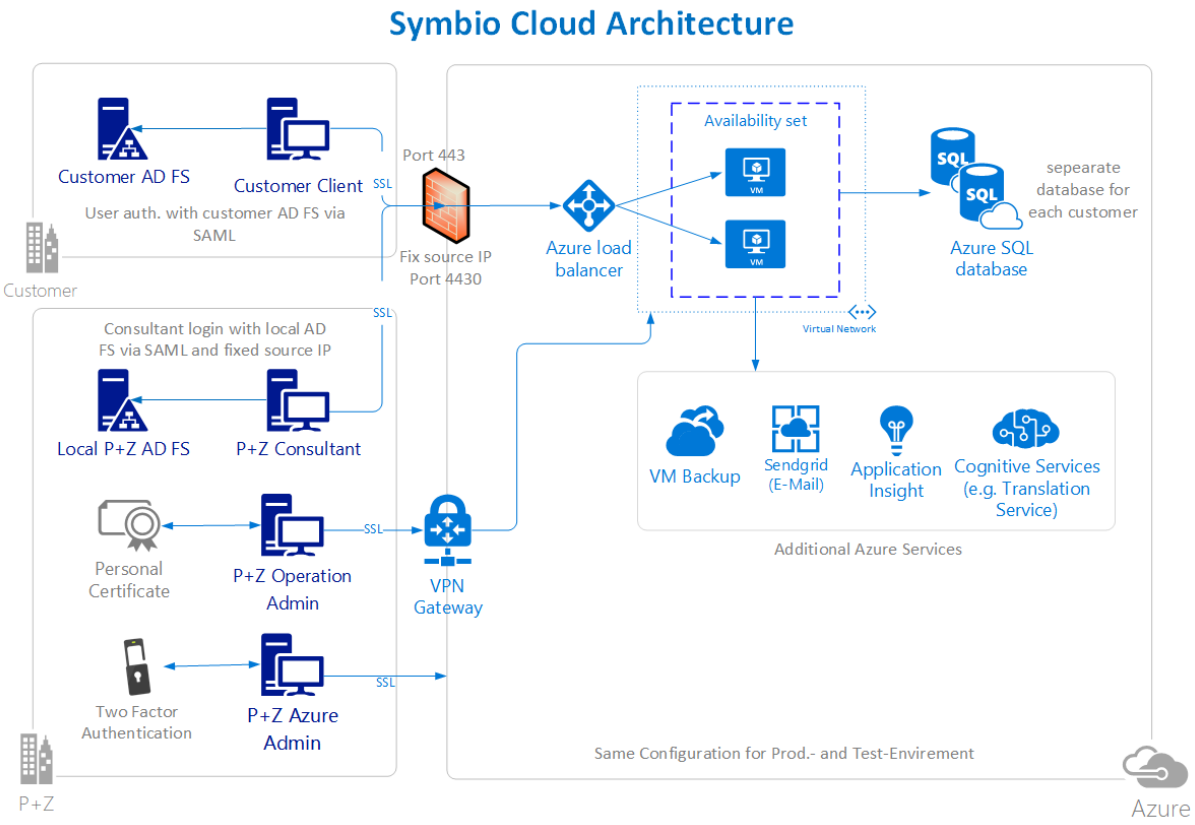


2.2 Symbio Azure Cloud Übersicht



2.3 Symbio Cloud Architecture Detailed

Das folgende Architekturbild zeigt den grundlegenden Aufbau der Symbio Cloud.



3 Symbio Cloud Varianten

3.1 Symbio Cloud Varianten

Als Kunde können Sie zwischen den folgenden Cloud Varianten auswählen:

3.1.1 Standard/ Professional Cloud

- Kein Symbio-Customizing möglich, d.h.
  - Symbio Standard-BPMN-Methode wird eingesetzt
  - Handbücher/Theme-Einstellungen sind allerdings manuell anpassbar
- Automatische Updates / Upgrades
- Pro Kunde eine eigene Azure SQL Datenbank

3.1.2 Enterprise Cloud

- Symbio-Customizing möglich
- Updates / Upgrades können verzögert eingestellt werden
- Pro Kunde eine eigene Azure SQL Datenbank
- Pro Kunde eine eigene Symbio Instanz

3.2 Symbio-Instanz-Einstellungen

Die Symbio-Instanz-Einstellungen lassen sich in der Exclusive-Cloud anpassen. Im Folgenden werden die Standardwerte beschreiben, diese gelten auch für die Standard-Cloud.

3.2.1 Rendering-Update-Intervall

Diagramme werden alle 30 Sekunden auf Aktualisierung im Hintergrund geprüft.

3.2.2 Free & Easy-DB

Datenbanken, die mit "Sandbox" beginnen, werden zu Spielwiesen, d.h. der Freigabe-Workflow ist in diesen Spielwiesen nicht aktiviert.

3.3 Logging und Tracing

3.3.1 Symbio

Jede Symbio-Instanz besitzt nur eine einzige Log-Datei, d.h. in der Standard-Cloud sieht ein Kunde auch die Log-Meldungen eines anderen Kunden und u. U. auch die URLs, falls Fehler aufgezeichnet worden sind. Diese Log-Dateien sind nur für Benutzer mit der Anwendungsrolle „Administrator" einsehbar.

1. Diese Log-Dateien sind 30 Tage online einsehbar.
2. Standardmäßig werden nur Fehler aufgezeichnet.
3. Zu Analysezwecken wie bspw. SAML-Anbindung für das Active Directory, kann das Logging-Level für eine kurze Zeit erhöht werden. Hier werden dann auch sensible Daten aufgezeichnet, z. B. (Claims aus Active Directory), aber niemals Passwörter.

3.3.2 IIS

Der Webserver IIS zeichnet standardmäßig die einzelnen Anfragen (IP, URL, Benutzer, usw.) auf. Die IIS-Logs sind nur für das Operation-Team einsehbar und können zu Performance-Analysen ausgewertet werden.

3.3.3 Windows

Windows zeichnet typische Log-Meldungen für Symbio als Anwendung auf, die nur für das Operation-Team einsehbar sind.

3.3.4 Datenbanken

In Azure SQL werden Log-Meldungen für jede Datenbank aufgezeichnet und bleiben nur für das Operation-Team einsehbar.

3.3.5 Performance

Mit Hilfe von Azure Application Insights werden neben typischen Web-Statistiken (Browser-Version, Geostatistik, usw.) Performance -Warnungen an das Operation-Team per Mail versendet, um ad-hoc Gegenmaßnahmen einzuleiten. Diese Gegenmaßnahmen können in sehr seltenen Fällen auch eine kurze Downtime verursachen.

3.4 Backup und Restore

3.4.1 Backup

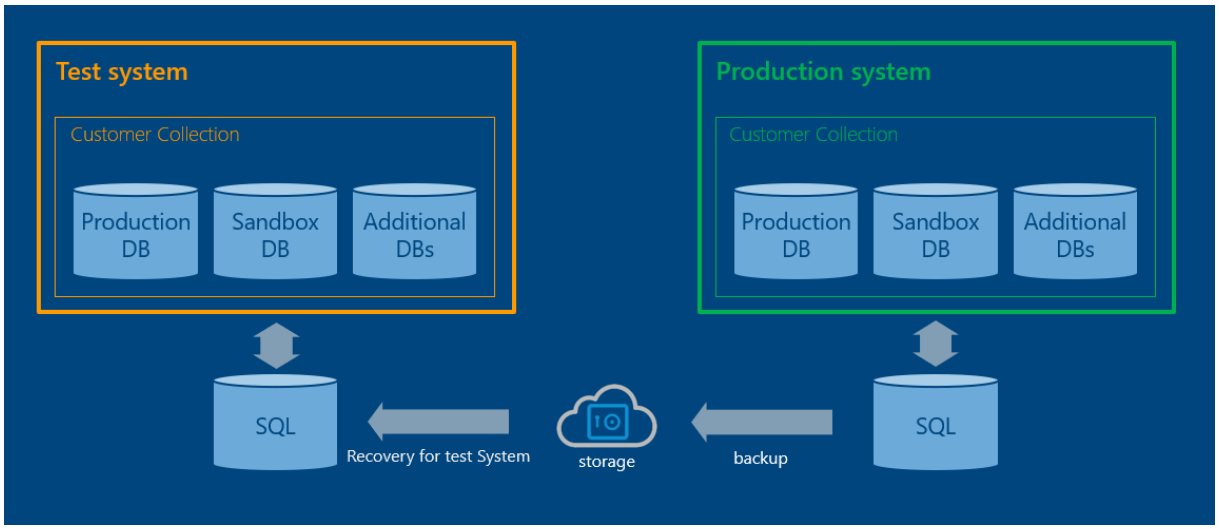
4. Azure SQL
    - Alle Symbio-Daten sind in SQL Datenbanken gesichert.
    - Datenbanken werden regelmäßig gesichert:
        - Voll-Backup wöchentlich
        - Differentiell alle 4 Stunden
        - Transaktions-Logs alle 5-10 Minuten
    - Datenbanksicherungen werden 35 Tage aufbewahrt.
    - Datenbanksicherungen von Datenbanken, die gelöscht wurden, werden 35 Tage nach Löschung der Datenbank, endgültig gelöscht.
    - Datenbanken und deren Backups werden verschlüsselt gesichert.
      Für die Verschlüsselung wird das Transparent Data Encryption (TDE) Verfahren angewendet mit vom Dienst verwaltete TDEs. Details zu diesem Verfahren finden Sie unter folgendem Link: https://aka.ms/sqlazuretde
5. Applikation Server
    - Es liegen keine Kundendaten auf dem Applikationsserver, außer Log-Daten.
    - Die virtuellen Maschinen werden nachts um 2 Uhr gesichert.
    - Die Festplatten werden mit BitLocker (AES 128 Bit) verschlüsselt.

3.4.2 Restore

Datenbank-Wiederherstellungen sind nach Absprache möglich oder werden vom Operation-Team bei fatalen Fehlern selbständig durchgeführt. Sollte ein Restore Ihrer Daten nötig sein, werden Sie vorher informiert.

3.4.3 Recoverytests

Recoverytests werden ca. alle 8 Wochen (pro Symbio Release) im Rahmen eines Upgrades durchgeführt. Hierbei werden die Daten vom Prod-System in das Test-System repliziert. Durch dieses Verfahren wird zyklisch überprüft, dass die Backups fehlerfrei funktionieren.



3.5 Update/Upgrade auf neue Versionen

Wann werden Updates/Upgrades eingestellt?

3.5.1 Hotfixes und Updates

Hotfixes werden automatisch während der Wartungsfenster eingespielt. Die Zeiten für das Wartungsfenster sind im SLA-Vertrag definiert.

3.5.2 Upgrades

Versions-Upgrades stehen ca. alle 8 Wochen zur Verfügung. In der Standard-Cloud werden Upgrades automatisch währen der Wartungsfenster eingespielt. In der Exclusive-Cloud werden diese nach Absprache eingespielt.

3.6 Relocate/Datenbank-Operationen

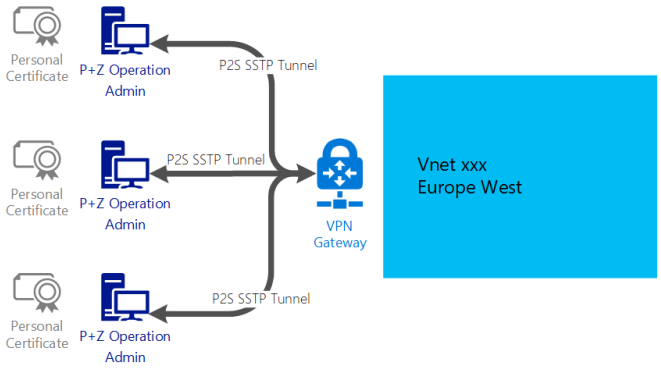
3.6.1 Kopieren einer Prod-Datenbank (Spielwiese)

Es ist generell möglich, eine Kopie Ihrer Produktiv-Datenbank in Symbio bereitzustellen. Bitte kontaktieren Sie uns.

3.7 Datenschutz und Sicherheitseinstellungen

3.7.1 Applikation Server

Der Zugriff auf die Applikation Server erfolgt durch das Operation-Team. Dieser Zugang ist nur über ein VPN über SSTP (Secure Socket Tunneling Protocol) mit persönlichen Zertifikat möglich. Das Zertifikat ist an den AD-Benutzer gebunden und Passwort-geschützt. Das Zertifikat ist vom Typ SHA256 mit einer Schlüssellänge von 2018 Zeichen gesichert.



Der Zugriff auf den eigentlichen Server wird über lokale Benutzer mit vordefiniertem Passwort realisiert. Die Sicherheit ist schon über den VPN-Tunnel gewährleistet.

3.7.1.1 Datenbank Authentifzierung (Azure SQL)

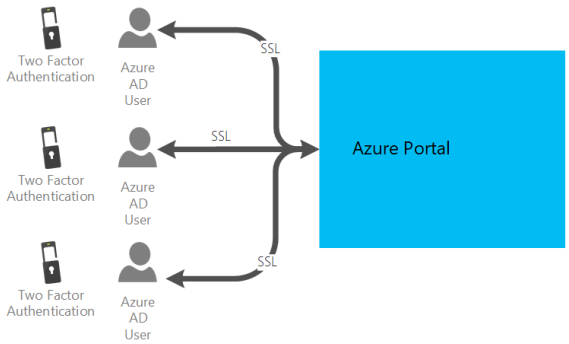
Die Authentifizierung zwischen Applikation-Server und Azure SQL wird über Azure AD-Benutzer realisiert. Auf dem Applikations-Server werden damit keine Passwörter im Klartext gespeichert. Pro Symbio-Instanz wird ein eigener Benutzer verwendet.

3.7.1.2 Verschlüsselung der Festplatten

Die Festplatten werden mit BitLocker (AES 128 Bit) verschlüsselt.
https://azure.microsoft.com/documentation/articles/storage-service-encryption/

3.7.2 Azure-Portal (inkl. Azure Services)

Der Zugriff auf das Azure Portal erfolgt durch das Operation-Team. Die Zugänge sind über Azure AD personifiziert. Die entsprechenden Azure AD-Benutzer sind mit einer Multi-Faktor-Authentifizierung gesichert. Auf vertrauenswürdigen Geräten muss die Multi-Faktor-Authentifizierung nach 30 Tagen erneuert werden.
Die Passwörter der Azure AD-Benutzer werden nach 180 Tagen erneuert.



3.7.3 Symbio-Zugriff

Alle Symbio-Anwender werden über Single-Sign-On via SAML authentifiziert.

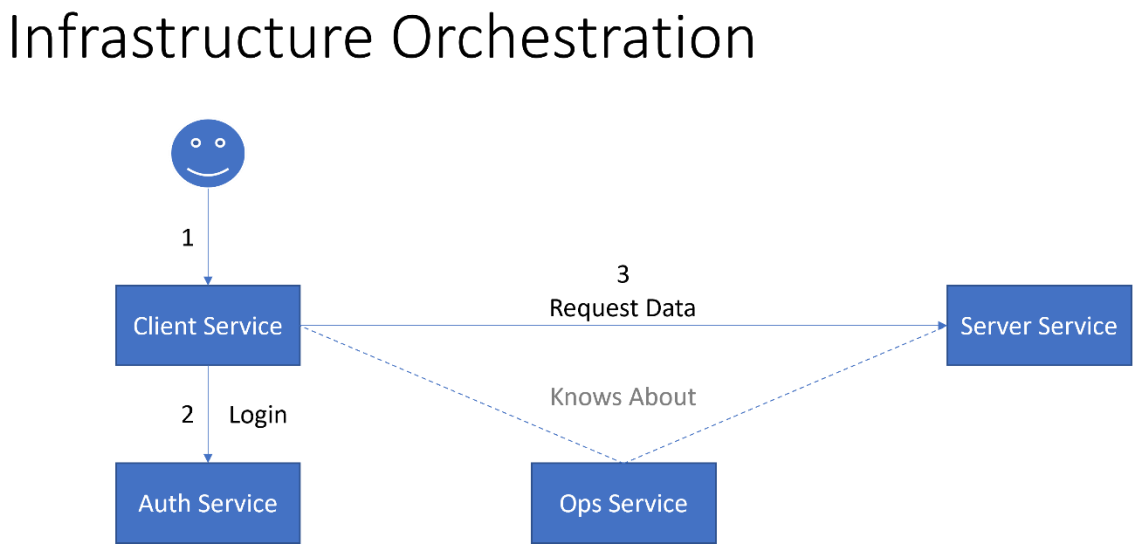
Über den gleichen Weg können nach Absprache mit dem Kunden auch Symbioworld Consultants auf die Daten zugreifen.

Hiermit ist sichergestellt, dass alle Verbindungen zwischen Client und Server SSL verschlüsselt sind.

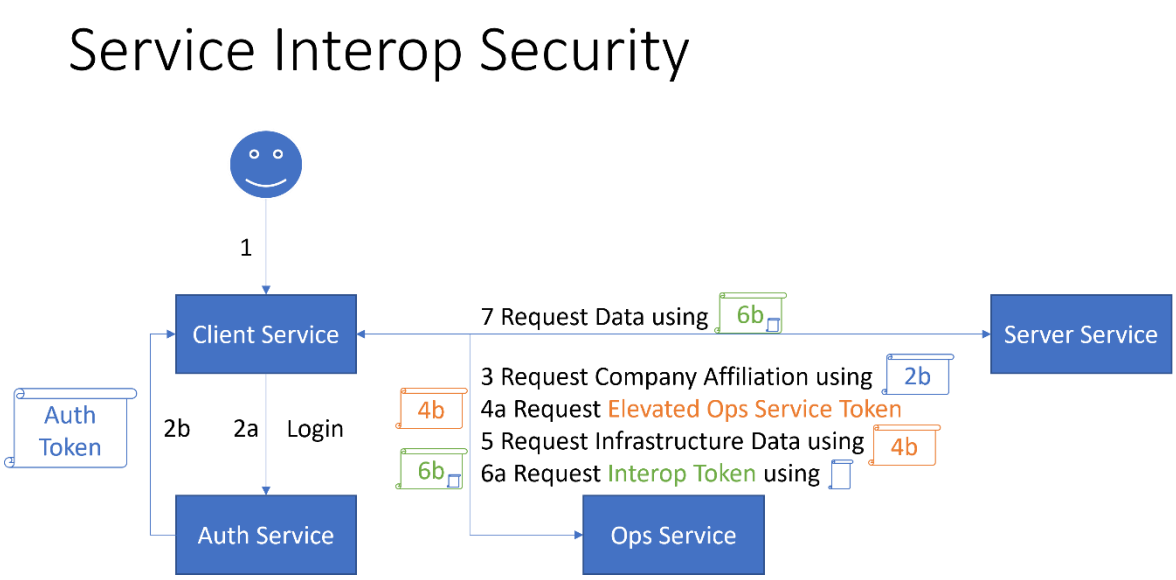
Details hierzu finden Sie hier.

3.7.4 Inter-Service (Interop) Sicherheit

Die Dienste im Symbio-Ökosystem werden durch den Symbio Operations Service (Ops Service) orchestriert, der über sie und den Kontext, in dem sie verwendet werden können, Bescheid weiß:



Während die Benutzeranmeldung bei einer Anwendung durch den Symbio Authorization Service (Auth Service) erleichtert wird, wird die Kommunikation zwischen den Diensten durch den Ops Service gesichert. Dies gilt insbesondere für Dienste, die Zugriff auf vertrauliche Daten gewähren (im Gegensatz zur Verarbeitung von nur bereitgestellten Daten):



Drei Arten von Token sind an der Sicherung des Zugriffs auf Anwendungen/Dienste beteiligt:

- **Auth-Tokens** identifizieren einen Benutzer und werden bei der Benutzeranmeldung ausgehändigt
- **Elevated Ops Service Tokens** identifizieren einen Dienst und können von einem Dienst angefordert werden, um Infrastrukturdaten im Ops Service anzufordern/zu manipulieren, auf die ein normaler Benutzer nicht zugreifen kann

- **Interop-Tokens** identifizieren einen Benutzer im Rahmen der Kommunikation zwischen Diensten und können von einem Client-Dienst für einen bestimmten Benutzer und einen Ziel-/Serverdienst angefordert werden; dieses Token wird nur ausgestellt, wenn auf den Zieldienst zugegriffen werden kann und der Zieldienst in der Lage ist, den zugehörigen Benutzer zu identifizieren und alle dienstspezifischen Berechtigungen anzuwenden

Diese Token sind JSON-Web-Token (https://jwt.io/) und werden auf der Grundlage von OpenID Connect und OAuth2-Prinzipien ausgestellt.

Herausgeber
Symbioworld GmbH
Einsteinring 41-43
85609 München
Tel.: +49 89 890635 – 0
Fax: +49 89 890635 – 55
E-Mail: info@symbioworld.com

Impressum
Für die Richtigkeit und Vollständigkeit der Darstellung/Abbildung im Dokument übernimmt Symbioworld GmbH keine Haftung. Die beschriebenen und möglichen Funktionalitäten der Software beziehen sich auf den jeweiligen Versionsstand. Kundenspezifische Anpassungen sind nicht enthalten. Die Informationen in diesem Dokument können sich zu jeder Zeit ändern. Symbioworld GmbH ist nicht verpflichtet über die Aktualisierungen des Dokumentes zu informieren.