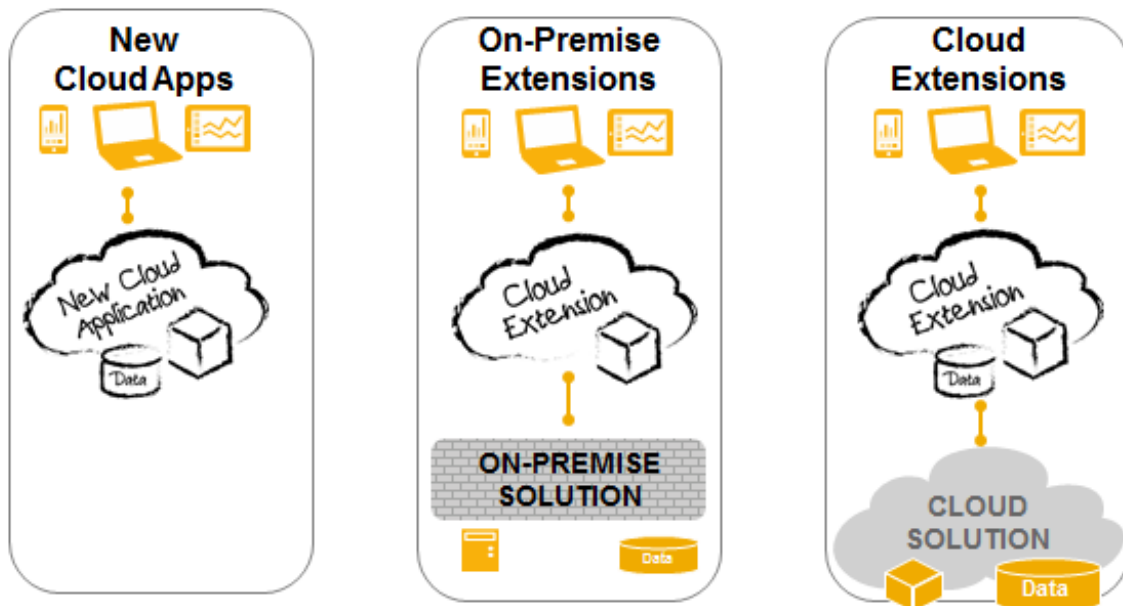


HANA CLOUD CONNECTOR



INHALTSVERZEICHNIS

Einleitung	3
Hana Cloud Connector	3
Was ist die Hana Cloud Plattform?	3
Warum mit dem Backend verbinden?	4
Hana Cloud Connector – Architektur Überblick.....	4
Datenaustausch – Die Szenarios.....	5
Anbindung von Cloud Applications an On-Premise Systeme.....	5
Anbindung des On-Premise Datenbank Tools an die Hana Cloud Plattform	6
Voraussetzungen zur Verwendung des Hana Cloud Connector.....	8
Alternative Anbindung via Reverse Proxy.....	9

EINLEITUNG

Dieses Dokument beschreibt die Verwendung des Hana Cloud Connectors im Überblick.

HANA CLOUD CONNECTOR

Der Hana Cloud Connector dient als Bindeglied zwischen On-Demand-Anwendungen in der SAP-HANA-Cloud-Plattform und bestehende On-Premise Systemen. Er kombiniert eine einfache Einrichtung mit einer klaren Konfiguration. Darüber hinaus können die Ressourcen, welche für die Cloud-Anwendungen in diesen Systemen verfügbar sein sollen, gesteuert werden.

Der Hana Cloud Connector wird als On-Premise-Agent in dem eigenen gesicherten Netzwerk installiert und fungiert als Reverse Invoke Proxy zwischen dem On-Premise-Netzwerk und der SAP HANA Cloud-Plattform. Aufgrund seiner Reverse Invoke Unterstützung, ist es nicht notwendig die Unternehmens-Firewall für den externen Zugriff aus der Cloud zu öffnen. Der Cloud Connector bietet eine fein abgestimmte Kontrolle über:

- On-Premise-Systemen und Ressourcen, die von Cloud-Anwendungen zugänglich sein sollen;
- Cloud-Anwendungen, welche den Cloud Connector nutzen soll.

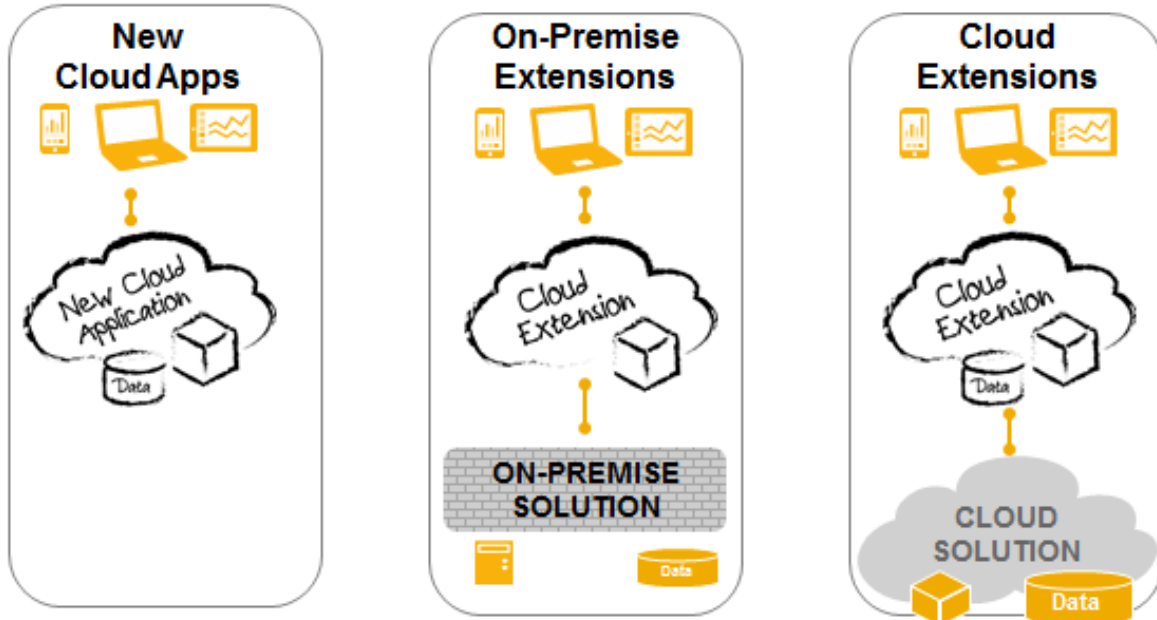
Das Tool baut automatisch die unterbrochenen Verbindungen wieder auf, bietet eine Audit-Protokollierung des eingehenden Datenverkehrs, Protokollierung aller Konfigurationsänderungen und kann in einem Hochverfügbarkeits-Setup ausgeführt werden.

Im Vergleich zum alternativen Ansatz einige Ports auf der Firewall zu öffnen und mit Reverse-Proxys in der DMZ Zugriff auf On-Premise Systeme zu etablieren, hat die Cloud Connector die folgenden Vorteile:

- Die Firewall des On-Premise-Netzwerks muss nicht angepasst werden.
- Der Cloud Connector unterstützt zusätzliche Protokolle, abgesehen von HTTP. Zum Beispiel unterstützt das RFC-Protokoll nativen Zugriff auf ABAP-Systeme um auch Funktionsbausteinen aufgerufen zu können.
- Der Hana Cloud Connector kann verwendet werden um on-Premise-Datenbank oder BI-Tools mit SAP HANA-Datenbanken in der Cloud zu verbinden.
- Der Hana Cloud Connector ermöglicht die Verwendung von Identity Propagation von Cloud-Nutzer zu On-Premise-Systeme in einer sicheren Weise.
- Der Hana Cloud Connector ist einfach zu installieren und zu konfigurieren.

Was ist die Hana Cloud Plattform?

Die SAP HANA Cloud Plattform ist ein In-Memory Platform-as-a-Service (PaaS) –Produkt. Unabhängige Softwareanbieter, Start-ups und Entwickler können SAP HANA verwenden, um HANA-basierte Cloud-Applikationen zu erstellen und zu testen. SAP HANA Cloud Plattform lässt sich außerdem nutzen, um Cloud- und On-Premise-Software zu erweitern. Das Angebot basiert auf einem Abonnement-Modell.



Die SAP HANA Cloud Plattform sollte nicht mit dem ähnlich benannten Angebot SAP HANA Enterprise Cloud verwechselt werden.

Mehr Infos: <https://hcp.sap.com/index.html>

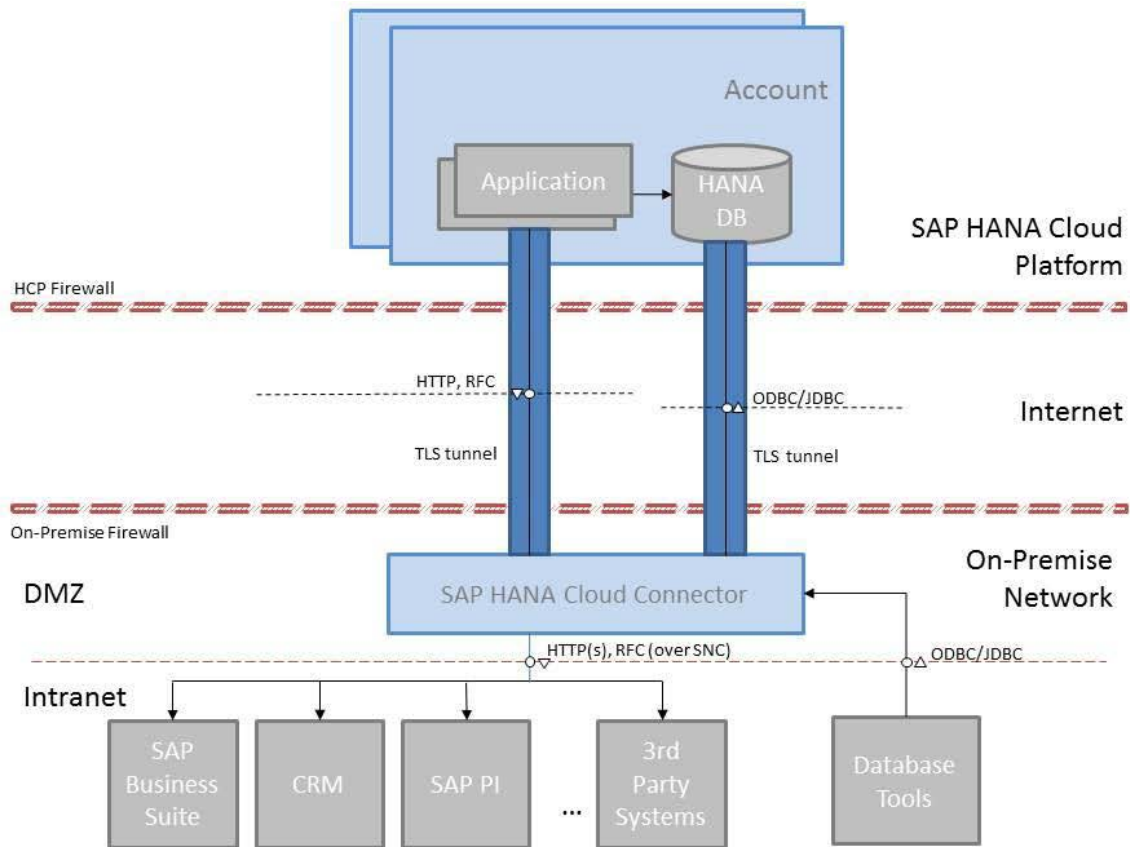
Warum mit dem Backend verbinden?

Typischerweise sind Daten und Business Logik in On-Premise SAP Systemen gespeichert. Es gibt eine Vielzahl von Fällen bei denen es Sinn macht, dass Apps aus der Cloud diese Daten verwenden sollten!

Beispiele: Stundenerfassung in der Cloud, KPIs auf dem Handy abrufen, Mobile Inbox und Freigabeszenarien.

Hana Cloud Connector – Architektur Überblick

Folgende Abbildung beschreibt die typische Architektur unter Verwendung der Hana Cloud Plattform und des Hana Cloud Connectors.



(Quelle: SAP / SAP HANA Cloud Connector: Security Whitepaper)

Der Hana Cloud Connector baut einen TLS Tunnel zur Cloud auf, durch den die Daten sicher über das Internet übertragen werden können.

Datenaustausch – Die Szenarios

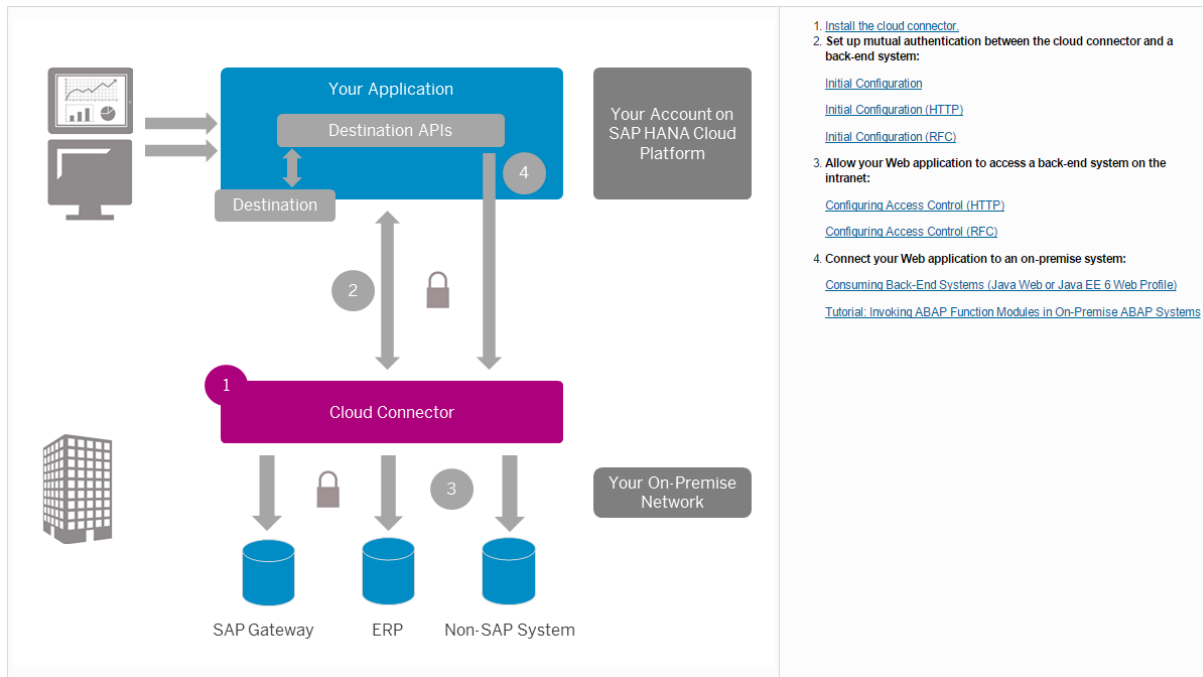
Der Hana Cloud Connector unterstützt zwei Szenarios für den Datenaustausch:

1. Anbindung von Cloud Applications an On-Premise Systeme
2. Anbindung der On-Premise Datenbank Tools an die Hana Cloud Plattform

Diese Szenarios sind im Folgenden beschrieben.

Anbindung von Cloud Applications an On-Premise Systeme

Dieses Szenario beschreibt wie Cloud Applikationen Zugriff auf Daten und Services aus dem Firmennetzwerk erhalten.



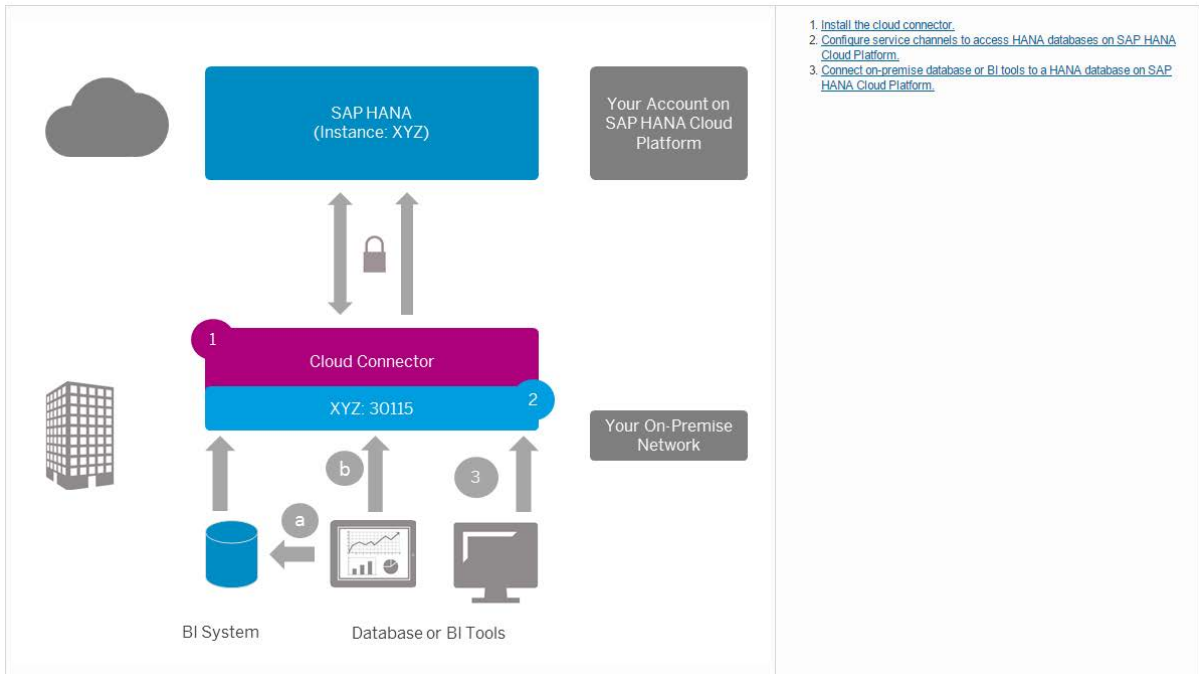
(Quelle: SAP / help.sap.com)

In der HCP wird eine Destination angelegt, die auf ein bestimmtes System verweist, welches im HCC konfiguriert ist. Dabei kann ein beliebiger Servername verwendet werden um die Namen im lokalen LAN zu schützen! Die Applikationen auf der HCP greifen dann auf genau diese Destination zu um die Daten aus dem On-Premise SAP System abzufragen.

Anbindung des On-Premise Datenbank Tools an die Hana Cloud Plattform

Dieses Szenario ermöglicht es On-Premise Datenbank Tools auch für die Datenbanken in der Hana Cloud Plattform zu verwenden, bzw. von On-Premise Apps auf diese Daten zuzugreifen

Schematische Darstellung:



(Quelle: SAP / help.sap.com)

Hier einige Szenarios wo eine Datenbankanbindung nützlich sein kann:

Connecting Cloud Databases

Why connecting cloud databases? (2)

Connecting Apps:

- Consume and manipulate data in the cloud database from on-premise apps
- Test new version of app on developer machine with real data before deploying

Connecting DB Tools:

- Introspection and manipulation of content and structures in the cloud database
- Supportability and debugging

Connecting Dev Tools:

- Model generation for object-relational persistence mapping frameworks
- Database refactoring

Connecting Replication Tools:

- Load cloud database with data from on-premise systems

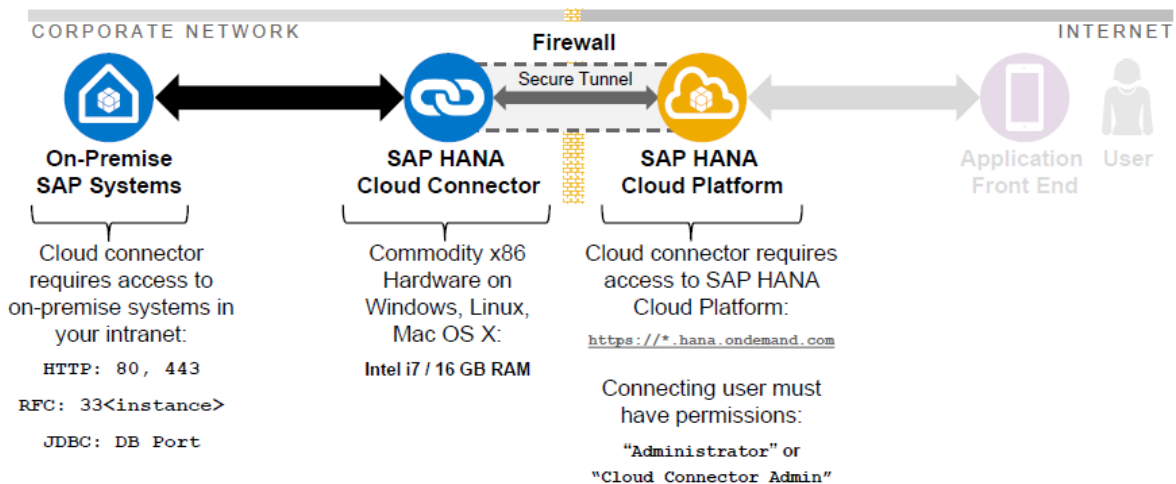


Voraussetzungen zur Verwendung des Hana Cloud Connector

- Der Hana Cloud Connector läuft auf gewöhnlicher Hardware auf den meisten Betriebssystemen.
- Der Hana Cloud Connector benötigt Zugriff auf das SAP System welches der Cloud zugänglich gemacht werden muss. Typischerweise der Cloud Connector ist im gleichen Netzwerk wie die SAP Systeme
- Das Backend System **muss nicht** aus dem Internet erreichbar sein!
- Es müssen **keine Ports auf der Firewall geöffnet** werden!
- Der Hana Cloud Connector benötigt Internet Zugriff um auf die Hana Cloud Plattform zugreifen zu können. Man kann bei Bedarf den Zugriff auch noch auf URL Basis einschränken.
- Nur User mit Admin Rechten können einen Cloud Connector einrichten

Cloud Connector

Prerequisites

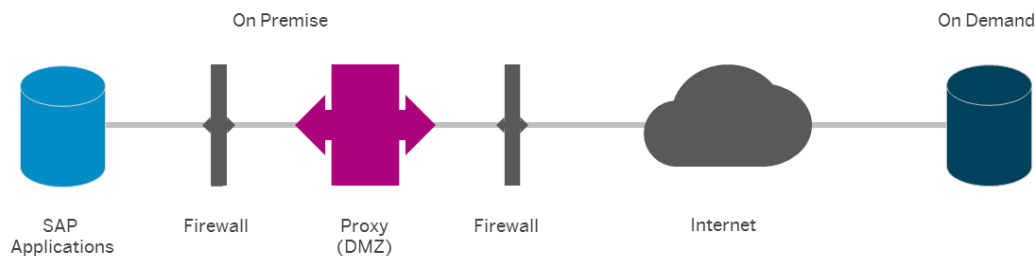


Alternative Anbindung via Reverse Proxy

Eine alternative Vorgehensweise im Vergleich zu der SSL VPN-Lösung des Hana Cloud Connector, ist es On-Premise-Dienste und Anwendungen über einen Reverse-Proxy für das Internet verfügbar zu machen. Für diese Methode gibt es typischerweise ein Reverse-Proxy-Setup in der "Demilitarisierten Zone" (DMZ) eines Kunden, die:

- Wirkt als Vermittler zwischen SAP-HANA-Cloud-Plattform und der On-Premise Systeme;
- Bietet die Dienste eines Application Delivery Controller (ADC)

Die folgende Abbildung zeigt die minimale Gesamtnetzwerktopologie dieses Ansatzes.



On-Premis-Services können dann über diesen Reverse-Proxy von der SAP HANA Cloud-Plattform wie andere HTTP-Dienste im Internet aufgerufen werden.

Vorteile

Je nach Szenario kann man von einem Reverse-Proxy profitieren. Ein Beispiel dafür ist die erforderliche Netzwerk-Infrastruktur (wie ein Reverse-Proxy und ADC-Dienste): wenn dies bereits in der Netzwerk Landschaft vorhanden ist, kann das Setup wieder verwendet werden um sich zur SAP HANA Cloud-Plattform zu verbinden. In diesem Fall gäbe es keine Notwendigkeit, neue Komponenten einzurichten und zu betreiben.

Nachteile

- Das Szenario bedingt, dass das SAP System aus dem Internet erreichbar ist.
- Der Reverse-Proxy-Ansatz verhindern nicht, dass die erreichbaren Services über das Internet allgemein zugänglich sind, was sie anfällig für Angriffe macht.
- SAP-proprietäres RFC-Protokoll wird nicht unterstützt, so dass eine Cloud-Anwendung nicht direkt auf RFC Services zugreifen kann.
- Zusätzlich unterstützt ein normaler Reverse-Proxy typischerweise keine Identity Propagation wodurch ein Single-Sign-On zwischen Cloud und On-Premise nur schwerer Umsetzbar ist.