Cloud Connector für SAP

Installation, Konfiguration und Betrieb

Kapitel 3
Einrichtung des Cloud Connectors

Der Cloud Connector ist neben SAP BTP das zentrale Element in hybriden Systemlandschaften. Er hilft Ihnen, SAP BTP sicher mit Ihrer On-Premise-Landschaft zu verbinden.

Dieses Kapitel führt Sie in die Installation und Konfiguration des Cloud Connectors ein. Das Kapitel beginnt mit Planungsüberlegungen, wie z. B. der Dimensionierung der Hardware. Anschließend werden Sie Schritt für Schritt durch den Installationsprozess geführt. Die Installation des Cloud Connectors ist generell nicht allzu kompliziert. Die eigentliche Herausforderung liegt in der Konfiguration, die in diesem Kapitel ausführlich behandelt wird.

Bevor wir auf die Installation des Cloud Connector eingehen, ist es sinnvoll, sich mit einigen wesentlichen Themen zu beschäftigen. Wir werden uns daher in Abschnitt 3.1, »Dimensionierung«, mit dem Thema Sizing beschäftigen. Danach geht es in Abschnitt 3.2, »Netzwerkzonen«, um die Positionierung des Cloud Connectors in Ihrem Unternehmensnetzwerk. Abschnitt 3.3, »Installation«, befasst sich dann mit der Installation des Cloud Connector. Nachdem der Cloud Connector installiert wurde, muss er auch entsprechend konfiguriert werden. Hierauf gehen wir in Abschnitt 3.4, »Konfiguration«, ein. In vielen Fällen ist es unerlässlich, dass der Cloud Connector hochverfügbar betrieben wird. Die erforderliche Konfiguration zeigen wir in Abschnitt 3.5, »Hochverfügbarkeit«.

3.1 Dimensionierung

Die Installation des Cloud Connectors ist eine einfache Angelegenheit. Allerdings reicht die Installation allein nicht aus, um eine angemessene Leistung zu gewährleisten. Sie müssen auch über die Dimensionierung (engl. Sizing) der zugrunde liegenden Hardware nachdenken. Einfach ausgedrückt ist der Sizing-Prozess die Dimensionierung der darunterliegenden Hardware. Sie umfasst die Festlegung von Eigenschaften wie Arbeitsspeicher, CPU-Leistung und Speicherplatz. Genau darum geht es in diesem Abschnitt. Im Gegensatz zu vielen anderen SAP-Produkten gibt es für den Cloud Connector keinen Quick Sizer. SAP empfiehlt jedoch drei verschiedene Dimensionen,

die auf Erfahrungswerten beruhen. Um es an dieser Stelle besonders einfach zu machen, hat man sich entschieden, für diese Dimensionen die bekannten T-Shirt-Größen zu verwenden: klein, mittel und groß (engl. Small, Medium, Large). Die Gesamtleistung des Cloud Connectors wird von vielen Faktoren beeinflusst. Dazu gehören die Anzahl der gehosteten Subaccounts, die verfügbare Bandbreite, die Latenzzeit zum Rechenzentrum und die verwendete *Java Virtual Machine* (JVM). Daher sind die Empfehlungen für die Dimensionierung nur eine Faustregel, da die tatsächliche Leistung stark von der jeweiligen Umgebung abhängt. Außerdem wird unterschieden, ob es sich bei der Installation um eine Master- oder eine Shadow-Instanz handelt. Die Installation kann in einer virtuellen oder physischen Maschine erfolgen. Eine virtuelle Maschine sollte sich auf einem Host befinden, der nicht übermäßig mit Ressourcen belastet ist.

Bei der Größenbestimmung ist die Ermittlung der Heap-Größe entscheidend. Ist sie zu klein für die Last, die durch den Cloud Connector läuft, führt die JVM häufiger vollständige Garbage Collections durch und blockiert die Verarbeitung des Cloud Connectors für mehrere Sekunden vollständig, was die Gesamtleistung massiv verlangsamt.

Garbage Collector

Der Garbage Collector dient als automatischer Speichermanager. Er verwaltet die Zuweisung und Freigabe von Speicher für eine Anwendung. Daher müssen Entwicklerinnen und Entwickler, die mit verwaltetem Code arbeiten, keinen zusätzlichen Code schreiben, um Aufgaben der Speicherverwaltung durchzuführen. Durch die automatische Speicherverwaltung können häufige Probleme der klassischen Programmierung vermieden werden, z. B. das Vergessen, ein Objekt freizugeben und dadurch ein Speicherleck zu verursachen, oder der Versuch, auf freigegebenen Speicher für ein Objekt zuzugreifen, welches bereits freigegeben wurde. Die JVM-Laufzeitumgebung verwendet einen großen Speicherpool, den sogenannten *Heap*, für die Objektzuweisung. Die JVM führt automatisch eine Garbage Collection durch, um den Heap aufzuräumen. Die Garbage Collection löscht Objekte, die nicht mehr verwendet werden, und schafft so Platz für neue Objekte. Wenn der Heap voll ist, wird ebenfalls eine Garbage Collection durchgeführt.

In den folgenden Abschnitten wird das Sizing für die Master- und Shadow-Installation detailliert beschrieben. Sie werden schnell feststellen, dass das Sizing im Vergleich zu anderen SAP-Systemen wie SAP NetWeaver sehr gering ist. Die heutigen Gaming-PCs sind mit mehr Leistung ausgestattet. Die Kosten für die Hardware werden sich in Grenzen halten. Daher sollten Sie die Hardware des Cloud Connectors unbedingt großzügig dimensionieren.

3.1.1 Dimensionierung der Master-Installation

Im Folgenden erläutern wir die allgemeinen Voraussetzungen für die Dimensionierung anhand der kleinen, mittleren und großen Größen für die Master-Installation. Bei den Empfehlungen für die einzelnen Größen handelt es sich um Mindestwerte; es kann jederzeit eine größere Größe gewählt werden. Im Allgemeinen gilt: Je mehr Anwendungen, Anwendungsinstanzen und Subaccounts verbunden sind, desto größer ist der Konkurrenzkampf um die begrenzten Ressourcen des Computers. Schauen wir uns nun jede Größe der Reihe nach an:

- Small Sizing
- Medium Sizing
- Large Sizing

Größe S (Small) wird empfohlen, wenn die erwartete Last gering ist und nur einige Subaccounts mit wenigen Anwendungen verbunden sind. Unter *geringer Last* versteht SAP bis zu 1 Million Anfragen pro Tag, mit geringer oder keiner Gleichzeitigkeit und einer geringen durchschnittlichen Anfragegröße. Darüber hinaus werden nur wenige Servicekanäle verwendet und nur geringe Datenmengen in Cloud-Systeme repliziert. Empfehlungen für die Dimensionierung sind in Tabelle 3.1 aufgeführt.

Komponente	Empfehlung für das Sizing
CPU	Zwei Cores, 2.6 GHz
Arbeitsspeicher (RAM)	4 GB
Heap	1 GB
Direct Memory	2 GB
Plattenplatz (engl. Disk Space)	10 GB

Tabelle 3.1 Small Sizing

Größe M (Medium) wird empfohlen, wenn die erwartete Last mittelhoch ist und mehrere Subaccounts mit mehreren Anwendungen verbunden sind. Mit *mittlerer Last* meint SAP bis zu 10 Millionen Anfragen pro Tag, mit mittlerer Gleichzeitigkeit und einer mittleren Durchschnittsgröße der Anfragen. Außerdem werden viele Servicekanäle genutzt und mittlere Datenmengen in Cloud-Systeme repliziert. Die Empfehlungen für das Sizing sind in Tabelle 3.2 aufgeführt.

Komponente	Empfehlung für das Sizing
CPU	Vier Cores, 3 GHz
Arbeitsspeicher (RAM)	16 GB
Heap	4 GB
Direct Memory	8 GB
Plattenplatz (engl. Disk Space)	20 GB

Tabelle 3.2 Medium Sizing

Größe L (Large) wird empfohlen, wenn die erwartete Last groß ist und viele Subaccounts mit vielen Anwendungen verbunden sind. Mit *großer Last* meint SAP mehr als 10 Millionen Anfragen pro Tag, mit hoher Gleichzeitigkeit und einer hohen durchschnittlichen Anfragegröße. Darüber hinaus werden viele Servicekanäle genutzt und große Datenmengen in Cloud-Systeme repliziert. Die Empfehlungen für die Dimensionierung sind in Tabelle 3.3 aufgeführt.

Komponente	Empfehlungen für das Sizing
CPU	Acht Cores, 3 GHz
Arbeitsspeicher (RAM)	32 GB
Heap	8 GB
Direct Memory	16 GB
Plattenplatz (engl. Disk Space)	40 GB

Tabelle 3.3 Large Sizing

3.1.2 Dimensionierung der Shadow-Installation

Eine Shadow-Installation kommt in der Regel nur ins Spiel, wenn etwas schief geht, und erfordert daher nicht zwangsläufig die gleiche Dimensionierung. In einem Failover-Setup übernimmt eine redundante Instanz die Rolle der Master-Instanz, wenn diese aus irgendeinem Grund ausfällt. Die Master-Instanz des Cloud Connectors wird als *Master* bezeichnet und die redundante Instanz als *Shadow*. Die Shadow-Instanz muss installiert und mit dem Master verbunden sein. Voraussetzung dafür ist, dass der Zeitraum, in dem sie die Master-Rolle übernimmt, zeitlich begrenzt ist. Im Schattenzustand ist der Ressourcenverbrauch sehr gering. Dies gilt insbesondere für Produktionsumgebungen, in denen normalerweise nur wenige Konfigurationsänderungen erforderlich sind. Daher empfiehlt SAP, dass die Größe des Shadow-Hosts

normalerweise kleiner sein kann als die des Master-Hosts. Wenn Sie jedoch das Risiko eines längeren Ausfalls des Master-Hosts mindern wollen, sollten Sie die Größe des Shadow-Hosts auf die Größe des Master-Hosts erhöhen.

Wir empfehlen, den Shadow-Host immer in der gleichen Größe wie den Master-Host zu dimensionieren. Wenn der Master-Host ausfällt, übernimmt der Shadow-Host die Aufgabe, aber wenn der Master-Host wieder verfügbar ist, schaltet der Shadow-Host nicht automatisch auf den Master-Host zurück. Das bedeutet, dass, wenn Sie Ihre Cloud-Connector-Landschaft nicht aktiv überwachen, die Shadow-Instanz möglicherweise über einen längeren Zeitraum hinweg weiterhin Nachrichten verarbeitet, bis Sie aktiv zum Master zurückschalten. Darüber hinaus bedeutet der Wechsel vom Master-Host zum Shadow-Host oder umgekehrt immer eine kurze Ausfallzeit. Während dieser Zeit können keine Nachrichten und Anfragen verarbeitet werden. Schauen wir uns nun die einzelnen Größen der Reihe nach an:

- Master-Größe S (klein)
- Master-Größe M (mittel)
- Master-Größe L (groß)

Wenn der Master-Host die Größe S hat, sollte auch der Shadow-Host die Größe S haben. Er kann auch auf einer virtuellen Maschine laufen, falls erforderlich. Die Größenordnung ist in Tabelle 3.4 angegeben.

Komponente	Empfehlungen für das Sizing
CPU	Zwei Cores, 2.6 GHz
Arbeitsspeicher (RAM)	4 GB
Heap	1 GB
Direct Memory	2 GB
Plattenplatz (engl. Disk Space)	10 GB

Tabelle 3.4 Small Sizing: Shadow gleich Master

Wenn der Hauptrechner die Größe M hat, sollte der Shadow-Host die Größe S haben und über den doppelten Speicher verfügen (siehe Tabelle 3.5).

Komponente	Empfehlungen für das Sizing
CPU	Zwei Cores, 2.6 GHz
Arbeitsspeicher (RAM)	8 GB

Tabelle 3.5 Small Sizing: Shadow mit doppeltem Speicher

Komponente	Empfehlungen für das Sizing
Heap	2 GB
Direct Memory	4 GB
Plattenplatz (engl. Disk Space)	10 GB

Tabelle 3.5 Small Sizing: Shadow mit doppeltem Speicher (Forts.)

Der Shadow-Host kann jedoch auch identisch mit dem Master-Host als Größe M dimensioniert werden (siehe Tabelle 3.6). Er kann auf einer virtuellen Maschine oder auf einem physischen Host laufen.

Komponente	Empfehlungen für das Sizing
CPU	Vier Cores, 3 GHz
Arbeitsspeicher (RAM)	16 GB
Heap	4 GB
Direct Memory	8 GB
Plattenplatz (engl. Disk Space)	20 GB

Tabelle 3.6 Medium Sizing: Shadow gleich Master

Wenn der Master-Host der Größe L entspricht, sollte der Shadow-Host die gleiche Größe haben wie ein Master-Host der Größe M (siehe Tabelle 3.7).

Komponente	Empfehlungen für das Sizing
CPU	Vier Cores, 3 GHz
Arbeitsspeicher (RAM)	16 GB
Heap	4 GB
Direct Memory	8 GB
Plattenplatz (engl. Disk Space)	20 GB

Tabelle 3.7 Medium-Sizing: Medium Shadow mit Large Master

Der Shadow-Host kann jedoch auch identisch mit dem Master-Host in der Größe L dimensioniert sein (siehe Tabelle 3.8). Er kann auf einer virtuellen Maschine oder auf einem physischen Host laufen.

Komponente	Empfehlungen für das Sizing
CPU	Acht Cores, 3 GHz
Arbeitsspeicher (RAM)	32 GB
Heap	8 GB
Direct Memory	16 GB
Plattenplatz (engl. Disk Space)	40 GB

Tabelle 3.8 Large Sizing: Shadow gleich Master

Je nach Sizing müssen Sie die Konfiguration möglicherweise anpassen, um die Gesamtleistung zu verbessern und die Hardwareressourcen angemessen zu nutzen. Dies ist in der Regel für eine mittlere oder große Installation relevant. Bei kleinen Installationen ist die Standardkonfiguration in der Regel ausreichend, um den Datenverkehr zu bewältigen. Dennoch sollten Sie die Konfiguration Ihrer Installation überprüfen. Die Konfiguration wird in Abschnitt 3.4, »Konfiguration«, ausführlich beschrieben.

3.2 Netzwerkzonen

Ein Netzwerk wird in der Regel in mehrere Netzwerkzonen oder Teilnetzwerke unterteilt. Dadurch lassen sich je nach Sicherheitsstufe der enthaltenen Komponenten spezifische Anforderungen abbilden. Eine solche Zone ist z. B. die *demilitarisierte Zone* (DMZ).

Demilitarisierte Zone

Ziel einer DMZ ist es, einer Organisation den Zugang zu nicht vertrauenswürdigen Netzwerken wie dem Internet zu ermöglichen und gleichzeitig sicherzustellen, dass ihr privates Netzwerk oder LAN sicher bleibt. Das DMZ-Netzwerk schützt das interne lokale Netzwerk einer Organisation (auch *Intranet* genannt) vor nicht vertrauenswürdigem Datenverkehr und bietet eine zusätzliche Sicherheitsebene. Eine DMZ ist in der Regel ein Subnetz, das zwischen dem öffentlichen Internet und privaten Netzwerken liegt. Die Server in der DMZ sind isoliert und haben nur begrenzten Zugang zum Intranet. Sie sind über das Internet zugänglich, jedoch nicht über das Intranet. Ein DMZ-Ansatz erschwert es einem Hacker, über das Internet direkt auf die Daten und internen Server eines Unternehmens zuzugreifen.

Sie können und müssen entscheiden, in welcher Netzwerkzone Sie den Cloud Connector installieren wollen. Der Cloud Connector kann entweder in der DMZ, wie in Abbildung 3.1 dargestellt, oder im Intranet eingerichtet werden.

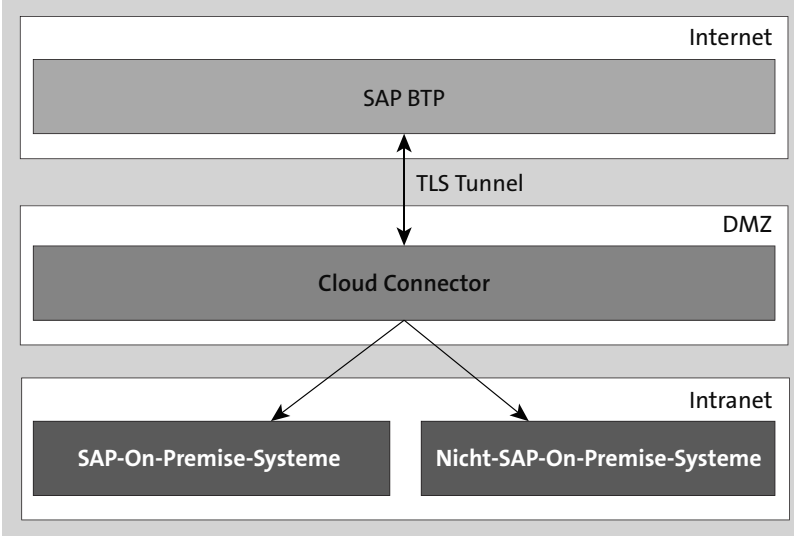


Abbildung 3.1 Cloud Connector in der DMZ

Für die Positionierung des Cloud Connectors in Ihrem Netzwerk gibt es zwei Voraussetzungen, die Sie erfüllen müssen:

- Der Cloud Connector muss einen Internetzugang zum Host der SAP-BTP-Region haben. Dies kann entweder direkt oder über einen HTTPS-Proxy erfolgen.
- Es muss ein direkter Zugang zu den internen Systemen bestehen, die über den Cloud Connector angesprochen werden sollen. Das bedeutet, dass es eine transparente Verbindung zwischen dem Cloud Connector und dem internen System gibt.

Vereinfacht gesagt, stellt der Cloud Connector eine *SSL-VPN-Lösung* (Secure Sockets Layer Virtual Private Network) dar, d. h., es wird ein VPN zwischen dem Cloud Connector und dem SAP-BTP-Subaccount aufgebaut. Ein alternativer Ansatz im Vergleich zu dieser VPN-Lösung besteht darin, Services und Anwendungen aus der On-Premise-Landschaft über einen Reverse-Proxy für das Internet zugänglich zu machen. Bei dieser Methode wird in der Regel ein Reverse-Proxy im Subnetz einer DMZ eingerichtet. Der Reverse-Proxy erfüllt mehrere Aufgaben. Er stellt die Services eines Application Delivery Controllers (ADC) zur Verfügung, um z. B. eingehenden Datenverkehr zu verschlüsseln, zu filtern, weiterzuleiten oder zu prüfen. Er fungiert als Vermittler oder »Man in the Middle« zwischen SAP BTP und den On-Premise-Services. On-Premise-Services, die über einen Reverse-Proxy zugänglich sind, können von SAP BTP wie andere im Internet verfügbare HTTP-Services genutzt werden.

Durch den Reverse-Proxy-Ansatz bleiben exponierte Services über das Internet generell zugänglich. Dies macht sie anfällig für Angriffe, insbesondere sind *Denial-of-Service-Angriffe* möglich. Um diese und andere Angriffe zu verhindern, müssen Sie in der DMZ und im Reverse-Proxy die höchsten Sicherheitsstandards implementieren. Das SAP-eigene RFC-Protokoll wird nur unterstützt, wenn WebSocket RFC für die Kommunikation mit dem ABAP-System verwendet werden kann. Daher kann nur das SAP-S/4HANA-System ab Version 1909 angesprochen werden.

Durch die Verwendung des Cloud Connectors werden die mit dem Reverse-Proxy verbundenen Probleme umgangen. Da der SSL-VPN-Tunnel zu SAP BTP über einen Reverse-Invoke-Ansatz aufgebaut wird, muss die DMZ oder externe Firewall eines Kundennetzwerks nicht für eingehenden Datenverkehr konfiguriert werden. Angriffe aus dem Internet sind nicht möglich.

3.3 Installation

Die Installation des Cloud Connectors ist grundsätzlich sehr einfach. Allerdings gibt es einige Voraussetzungen, die Sie im Vorfeld prüfen sollten. Eine Voraussetzung ist die Verwendung eines von SAP unterstützten Betriebssystems. Die folgenden Betriebssysteme werden unterstützt:

- Red Hat Enterprise Linux (x86/64 und PowerPC)
- SUSE Linux Enterprise Server (x86/64 und PowerPC)
- Windows-Server
- Windows 11
- macOS
  Beachten Sie, dass Sie macOS nicht für produktive Szenarien verwenden sollten.

Der Cloud Connector ist eine Java-Anwendung, die zur Ausführung eine JVM benötigt. Die Anwendung ist als Webanwendung implementiert und verwendet *Apache Tomcat* als Laufzeitumgebung. Der Cloud Connector benötigt mindestens *JVM 8* in allen derzeit unterstützten Versionen. Ab Cloud Connector Version 2.14.0 ist eine SAP JVM der Version 11 erforderlich; Cloud Connector Version 2.15.0 erfordert JVM Version 17.

Java Virtual Machine

Die JVM lädt den Java-Bytecode, prüft ihn und führt ihn aus. Sie wird als *Interpreter* bezeichnet und ist somit der Kern der Java-Programmiersprache, da sie die Java-Programme ausführt. Sie ist plattformabhängig und führt viele Funktionen aus, einschließlich Speicherverwaltung und Sicherheit.

Der Cloud Connector muss in der Lage sein, eine Internetverbindung zu den SAP-Connectivity-Service-Hosts herzustellen. Dies ist das Gegenstück zum Cloud Connector in SAP BTP. Der Cloud Connector verbindet sich aktiv mit dem SAP-Connectivity-Service. Alle Verbindungen zu den Hosts sind TLS-basiert und werden über Port 443 hergestellt. Das bedeutet, dass Ihre Firewall eine ausgehende Verbindung über Port 443 zu SAP BTP zulassen muss. Sie haben auch die Möglichkeit, ausgehende Verbindungen auf die IP-Adressen der verwendeten Rechenzentren zu beschränken. Wir führen die IP-Adressen hier bewusst nicht auf, da sie sich häufig ändern. Die aktuell gültige Liste finden Sie in der Dokumentation des Cloud Connectors.

Wenn Sie den Cloud Connector in einem von den Backend-Systemen isolierten Netzwerksegment – beispielsweise der DMZ – installieren, müssen Sie sicherstellen, dass die exponierten Hosts mit den zugehörigen Ports netzwerkfähig sind. Das bedeutet, dass Sie in der Firewall die Ports für den eingehenden Datenverkehr (incoming) öffnen müssen.

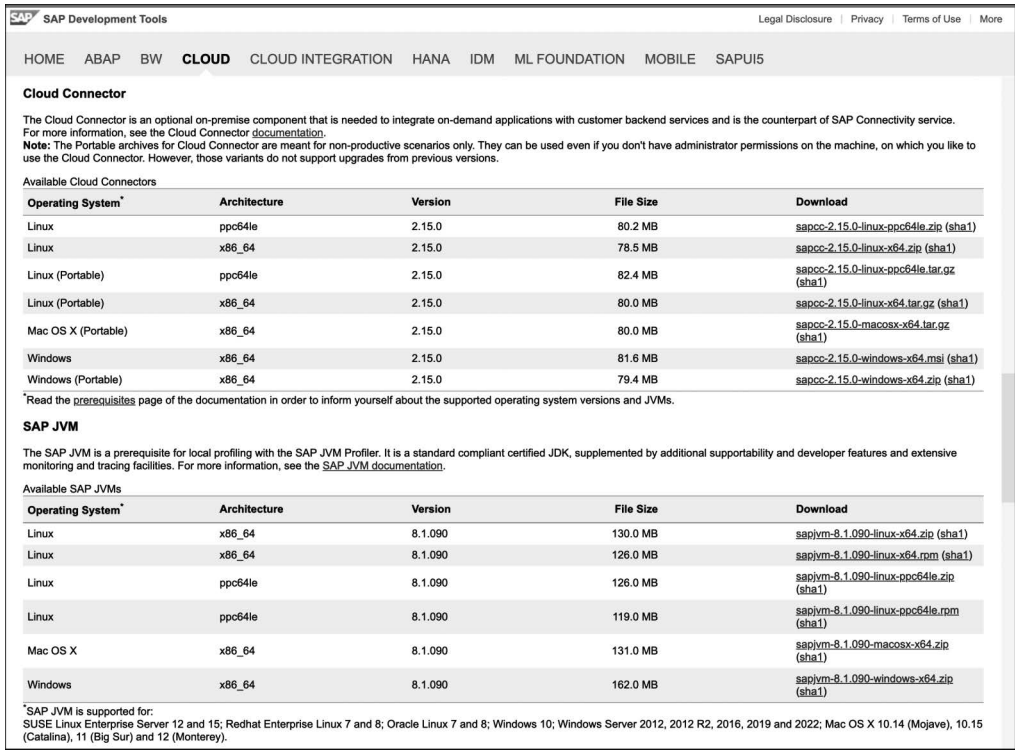
Nachdem Sie alle Voraussetzungen in Ihrer Systemlandschaft erfüllt haben, kann der Cloud Connector installiert werden. Dazu muss der Cloud Connector von *https://tools.hana.ondemand.com/* heruntergeladen werden. Im Gegensatz zu den meisten anderen SAP-Produkten wird der Cloud Connector nicht über den *SAP Service Marketplace* bezogen. Sie benötigen also keinen Benutzer im SAP Service Marketplace, um ihn herunterzuladen. Auf der gleichen Seite, von der der Cloud Connector bezogen werden kann, bietet SAP auch die SAP JVM zum Download an (siehe Abbildung 3.2).

Wie Sie in Abbildung 3.2 sehen können, steht der Cloud Connector auch in einer portablen Version zum Download bereit. Dies ist eine Version, die nur entpackt werden muss und dann direkt von der Kommandozeile aus gestartet werden kann. Bitte beachten Sie, dass für die Installation keine Administrator- oder Root-Rechte erforderlich sind. Sie können mehrere Instanzen auf demselben Host auf verschiedenen Ports laufen lassen. Die portable Version hat die folgenden Einschränkungen:

- Sie ist nur für Nicht-Produktionsszenarien gedacht.
- Sie unterstützt kein automatisches Upgrade-Verfahren. Um eine portable Installation zu aktualisieren, müssen Sie die aktuelle Installation löschen, die neue Version extrahieren und sie dann neu konfigurieren.
- Die Umgebungsvariable `JAVA_HOME` ist beim Starten der Instanz relevant und muss daher korrekt gesetzt werden.
- Sie können es nicht im Hintergrund als Windows-Dienst oder Linux-Daemon laufen lassen.

Die anderen, nicht portablen Versionen, auch Installer-Versionen genannt, werden mit einem Installationsprogramm geliefert, das den Cloud Connector auch als Ser-

vice im zugrunde liegenden Betriebssystem einrichtet. Dies erfordert Administrator- oder Root-Rechte für die Installation und ermöglicht es, den Cloud Connector so einzurichten, dass er als Windows-Dienst oder Linux-Daemon im Hintergrund läuft. Sie können die Installationsversion problemlos aktualisieren, wobei alle Konfigurationen und Anpassungen, die Sie vorgenommen haben, erhalten bleiben.



SAP Development Tools — Legal Disclosure | Privacy | Terms of Use | More

HOME ABAP BW **CLOUD** CLOUD INTEGRATION HANA IDM ML FOUNDATION MOBILE SAPUI5

Cloud Connector

The Cloud Connector is an optional on-premise component that is needed to integrate on-demand applications with customer backend services and is the counterpart of SAP Connectivity service.
For more information, see the Cloud Connector documentation.
Note: The Portable archives for Cloud Connector are meant for non-productive scenarios only. They can be used even if you don't have administrator permissions on the machine, on which you like to use the Cloud Connector. However, those variants do not support upgrades from previous versions.

Available Cloud Connectors

Operating System*	Architecture	Version	File Size	Download
Linux	ppc64le	2.15.0	80.2 MB	sapcc-2.15.0-linux-ppc64le.zip (sha1)
Linux	x86_64	2.15.0	78.5 MB	sapcc-2.15.0-linux-x64.zip (sha1)
Linux (Portable)	ppc64le	2.15.0	82.4 MB	sapcc-2.15.0-linux-ppc64le.tar.gz (sha1)
Linux (Portable)	x86_64	2.15.0	80.0 MB	sapcc-2.15.0-linux-x64.tar.gz (sha1)
Mac OS X (Portable)	x86_64	2.15.0	80.0 MB	sapcc-2.15.0-macosx-x64.tar.gz (sha1)
Windows	x86_64	2.15.0	81.6 MB	sapcc-2.15.0-windows-x64.msi (sha1)
Windows (Portable)	x86_64	2.15.0	79.4 MB	sapcc-2.15.0-windows-x64.zip (sha1)

*Read the prerequisites page of the documentation in order to inform yourself about the supported operating system versions and JVMs.

SAP JVM

The SAP JVM is a prerequisite for local profiling with the SAP JVM Profiler. It is a standard compliant certified JDK, supplemented by additional supportability and developer features and extensive monitoring and tracing facilities. For more information, see the SAP JVM documentation.

Available SAP JVMs

Operating System*	Architecture	Version	File Size	Download
Linux	x86_64	8.1.090	130.0 MB	sapjvm-8.1.090-linux-x64.zip (sha1)
Linux	x86_64	8.1.090	126.0 MB	sapjvm-8.1.090-linux-x64.rpm (sha1)
Linux	ppc64le	8.1.090	126.0 MB	sapjvm-8.1.090-linux-ppc64le.zip (sha1)
Linux	ppc64le	8.1.090	119.0 MB	sapjvm-8.1.090-linux-ppc64le.rpm (sha1)
Mac OS X	x86_64	8.1.090	131.0 MB	sapjvm-8.1.090-macosx-x64.zip (sha1)
Windows	x86_64	8.1.090	162.0 MB	sapjvm-8.1.090-windows-x64.zip (sha1)

*SAP JVM is supported for:
SUSE Linux Enterprise Server 12 and 15; Redhat Enterprise Linux 7 and 8; Oracle Linux 7 and 8; Windows 10; Windows Server 2012, 2012 R2, 2016, 2019 and 2022; Mac OS X 10.14 (Mojave), 10.15 (Catalina), 11 (Big Sur) and 12 (Monterey).

Abbildung 3.2 Cloud Connector und JVM herunterladen

Im Folgenden zeigen wir Ihnen, wie Sie den Cloud Connector auf einem Windows-Betriebssystem installieren. Um den Cloud Connector zu installieren, müssen Sie die Laufzeitbibliotheken von Microsoft Visual Studio C++ 2013 installieren (Dateiname **vcredist_x64.exe**). Informationen hierzu finden Sie in SAP-Hinweis 2493763.

Die Installation auf Linux-Betriebssystemen funktioniert prinzipiell auf ähnliche Weise. Nachdem Sie den Cloud Connector heruntergeladen und auf den Rechner übertragen haben, auf dem er installiert werden soll, kann der Installer im Datei-Explorer durch Doppelklick auf die MSI-Datei gestartet werden. Sie werden von einem Assistenten durch die Installation geführt, wie in Abbildung 3.3 dargestellt. Im ersten Schritt werden die Voraussetzungen geprüft. Wenn kein Fehler auftritt, können Sie auf **Next** klicken.

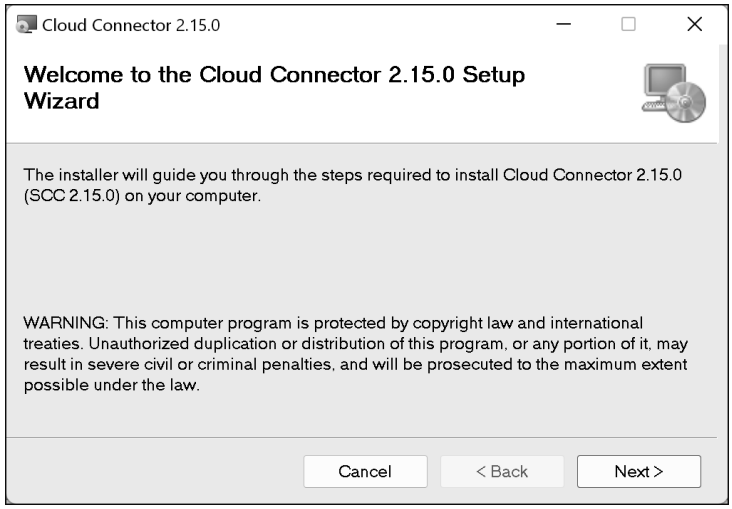


Abbildung 3.3 Installationsanweisungen

Im nächsten Schritt müssen Sie das Installationsverzeichnis auswählen (siehe Abbildung 3.4). Klicken Sie dann auf **Next**.

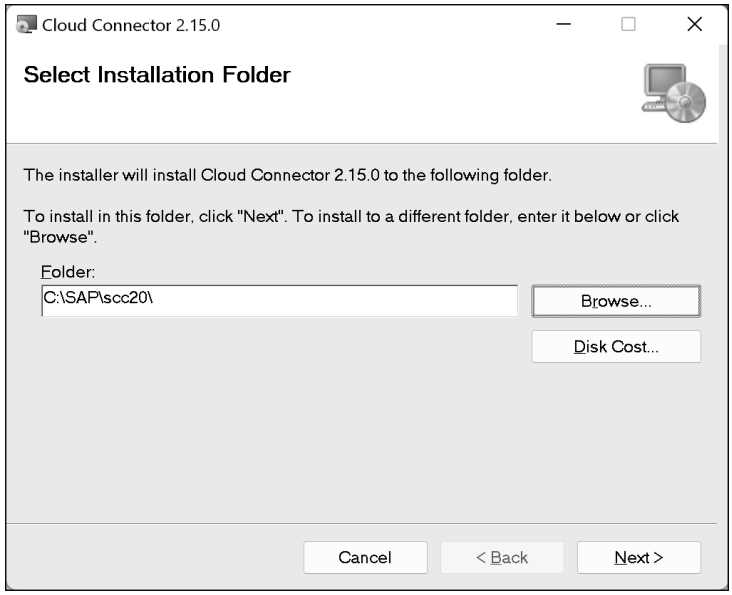


Abbildung 3.4 Installationsverzeichnis wählen

Danach haben Sie die Möglichkeit, den vom Cloud Connector verwendeten Port anzupassen. Standardmäßig wird der Cloud Connector auf Port 8443 installiert (siehe Abbildung 3.5). Klicken Sie dann auf **Next**.

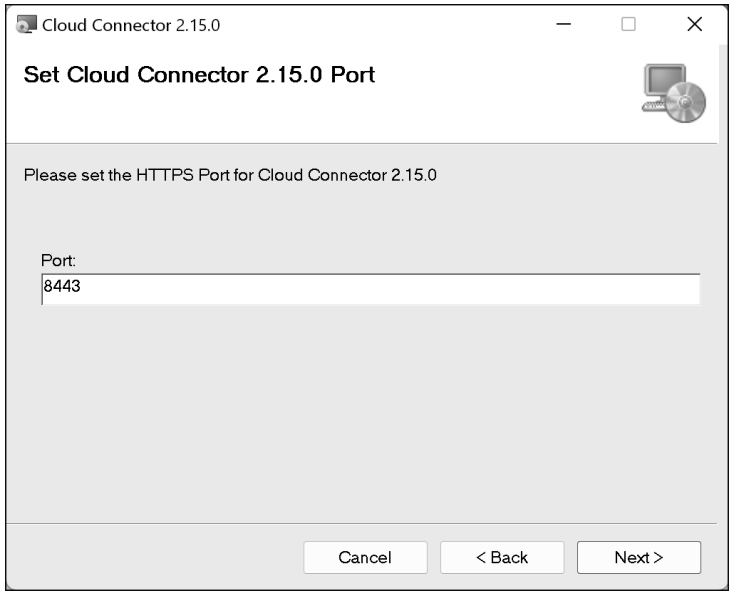


Abbildung 3.5 Portnummer auswählen

Sie müssen nun das passende Installationsverzeichnis des JDK auswählen (siehe Abbildung 3.6). Stellen Sie sicher, dass Sie eine von SAP unterstützte Version verwenden.

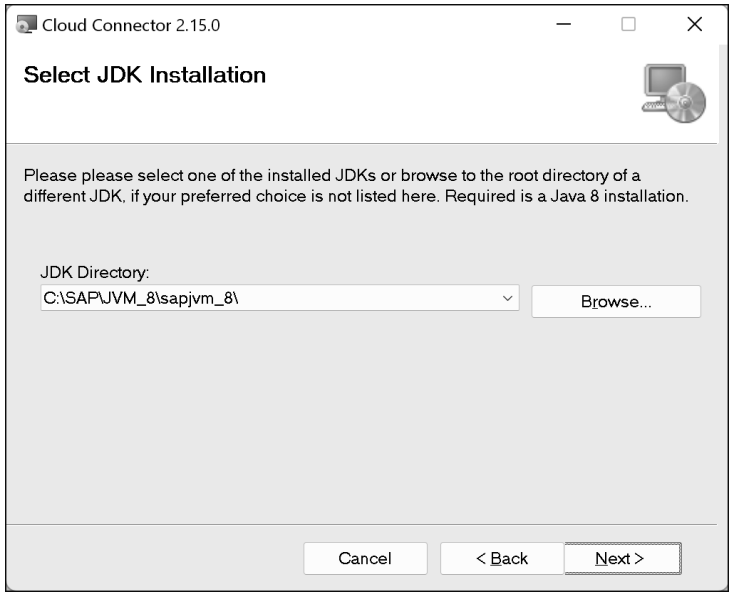


Abbildung 3.6 JDK-Verzeichnis auswählen

Unterstützte Versionen

Die unterstützten Versionen finden Sie in der Dokumentation des SAP-Connectivity-Service im Abschnitt **Cloud Connector • Installation • Prerequisites**. Zum Zeitpunkt der Erstellung dieses Buches ist diese Dokumentation unter *http://s-prs.de/v970702* verfügbar.

Wenn Sie fertig sind, klicken Sie auf **Next**.

Sie haben nun die Möglichkeit, festzulegen, ob der Cloud Connector sofort nach erfolgreicher Installation gestartet werden soll (siehe Abbildung 3.7). Klicken Sie dann auf **Next**.

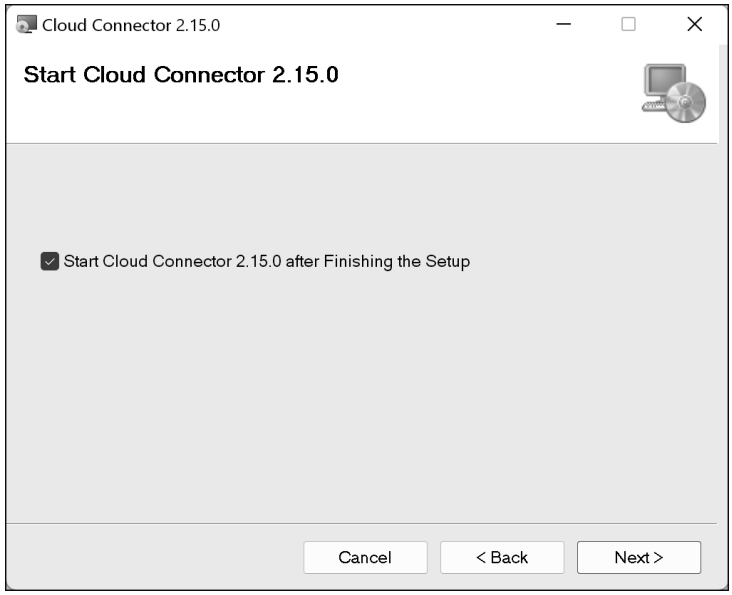


Abbildung 3.7 Starten des Cloud Connectors nach erfolgreicher Installation

Abschließend müssen Sie noch einmal bestätigen, dass Sie die Installation starten wollen (siehe Abbildung 3.8). Klicken Sie dann auf **Next**, um die Installation zu starten.

Nachdem die Installation gestartet wurde, sehen Sie den Status der Installation (siehe Abbildung 3.9). Normalerweise sollten zu diesem Zeitpunkt keine Fehler auftreten.

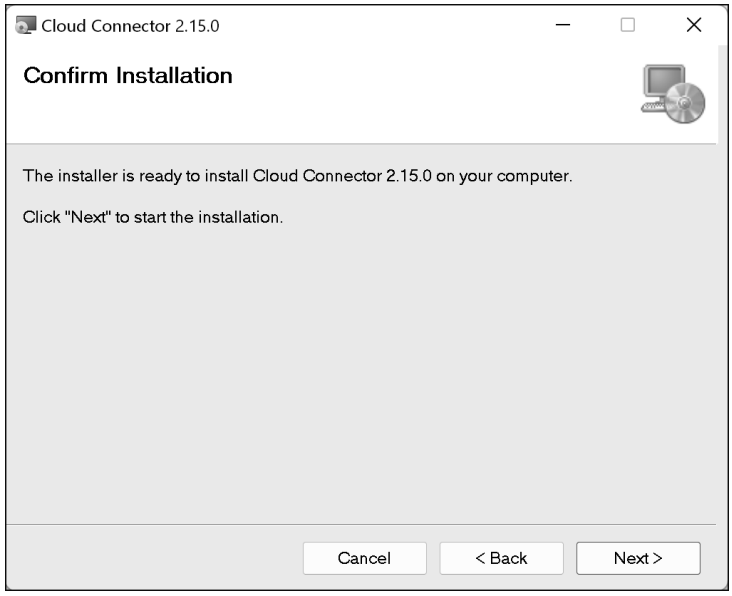


Abbildung 3.8 Installation starten

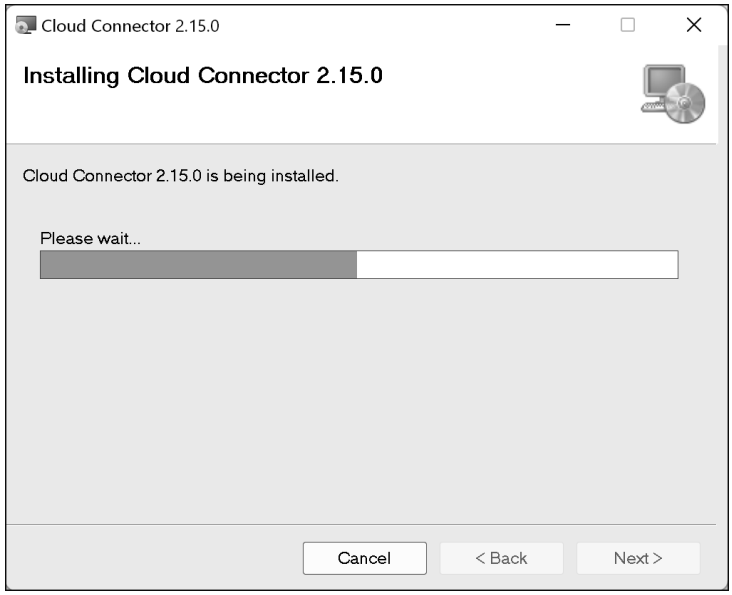


Abbildung 3.9 Fortschritte bei der Installation

Nach erfolgreicher Installation werden Sie über den Abschluss der Installation informiert (siehe Abbildung 3.10). Schließen Sie den Dialog, indem Sie auf **Close** klicken.

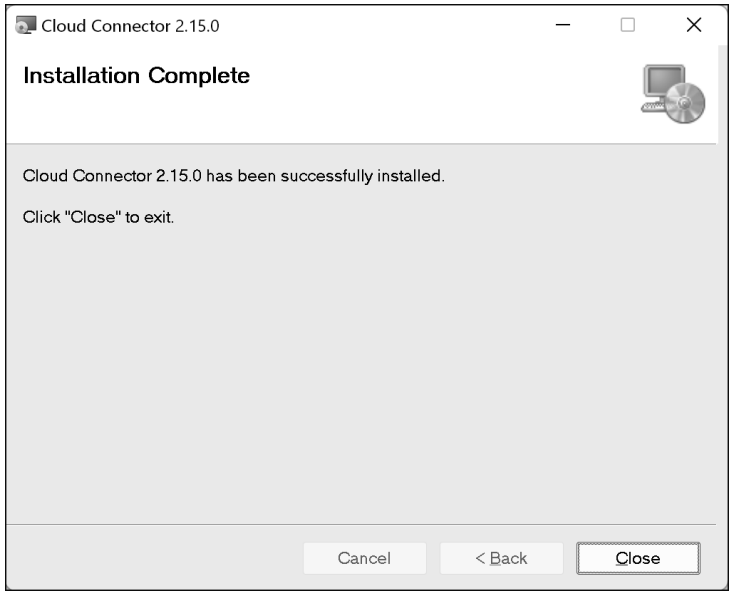


Abbildung 3.10 Installation abgeschlossen

Nach Abschluss der Installation sehen Sie die in Abbildung 3.11 dargestellte Verzeichnisstruktur. Die wichtigsten Dateien im Installationsverzeichnis sind die folgenden:

- **go.bat (.sh)**
  Damit können Sie den Cloud Connector manuell starten.
- **changeport.bat (.sh)**
  Hiermit können Sie den vom Cloud Connector verwendeten Port ändern.
- **useFileUserStore.bat (.sh)**
  Wenn Ihre LDAP-Einstellungen nicht wie erwartet funktionieren, können Sie hiermit zum dateibasierten Benutzerspeicher zurückkehren.
- **changeAuditLogPath.bat (.sh)**
  Ab Cloud Connector 2.14 können Sie damit Audit-Protokolle an einen anderen Ort verschieben. Der Standardspeicherort ist das Verzeichnis **log/audit**.
- **changeLogAndTracePath.bat (.sh)**
  Ab Cloud Connector 2.14 können Sie damit Trace-Dateien an einen anderen Ort verschieben. Die JVM-bezogenen Dateien bleiben im Standard Log (Default Log Location).

An dieser Stelle sollten wir auch erwähnen, dass der Cloud Connector keine Datenbank benötigt. Das bedeutet, dass die gesamten Konfigurations-, Protokoll- und Trace-Dateien lokal auf dem Dateisystem des Cloud Connectors gespeichert werden. Daher sollten Sie sicherstellen, dass das Installationsverzeichnis in Ihrem Backup ent-

halten ist. Allerdings sollten Sie auch den Zugriff auf das Verzeichnis entsprechend Ihren Anforderungen einschränken. Besonderes Augenmerk sollte auf die Protokoll- und Trace-Dateien gelegt werden.

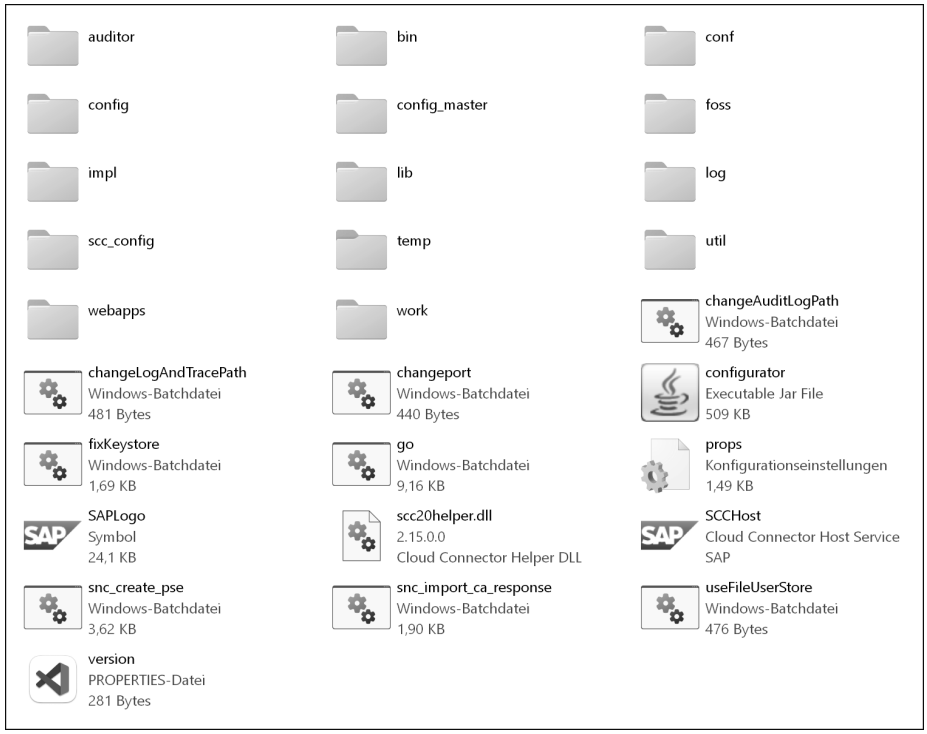


Abbildung 3.11 Verzeichnisstruktur

3.4 Konfiguration

Nachdem der Cloud Connector installiert wurde, kann die Administrationsoberfläche des Cloud Connectors in einem Browser Ihrer Wahl geöffnet werden. Als Hostname ist der Hostname des Servers zu verwenden, auf dem der Cloud Connector installiert wurde. Standardmäßig wird der Port 8443 verwendet, aber Sie haben die Möglichkeit, den Port während der Installation zu ändern, wie im vorherigen Abschnitt beschrieben. In Abschnitt 3.4.1, »Initiale Schritte«, werden wir uns die ersten Schritte ansehen, die bei der Ersteinrichtung des Cloud Connectors befolgt werden müssen. Danach zeigen wir Ihnen in Abschnitt 3.4.2, »Konfiguration der Benutzeroberfläche«, wie Sie den Anmeldebildschirm des Cloud Connectors anpassen können. Dort erfahren Sie auch, wie Sie den Benutzernamen und das Passwort des Cloud-Connector-Benutzers ändern können. Darüber hinaus erfahren Sie, wie Sie das UI-Zertifikat austauschen, damit die Administration beim Zugriff auf den Cloud Connec-

tor eine verschlüsselte Verbindung mit einem vertrauenswürdigen Zertifikat verwenden kann. In Abschnitt 3.4.3, »Cloud-Konfiguration«, zeigen wir einige Optionen, die bei der Verbindung mit SAP BTP verfügbar sind. Sie erfahren, wie Sie einen Proxy-Server einrichten und wo Sie den Cloud-Benutzerspeicher einrichten, damit sich Cloud-Benutzer anhand eines LDAP authentifizieren können. Dann erfahren Sie, wie Sie benutzerdefinierte Regionen einrichten, falls das von Ihnen verwendete Rechenzentrum noch nicht vom Cloud Connector unterstützt wird. Im nächsten Abschnitt 3.4.4, »On-Premise-Konfiguration«, erfahren Sie alles, was Sie für die Konfiguration der Verbindung zu Ihren On-Premise-Systemen wissen müssen. In Abschnitt 3.4.5, »Reporting-Konfiguration«, erfahren Sie, an welcher Stelle die Verbindung zum SAP Solution Manager konfiguriert wird. In Abschnitt 3.4.6, »Advanced-Konfiguration«, schließlich erfahren Sie, welche erweiterten Konfigurationsmöglichkeiten Ihnen zur Verfügung stehen.

3.4.1 Initiale Schritte

Wenn Sie sich zum ersten Mal anmelden, werden Sie feststellen, dass eine Sicherheitswarnung angezeigt wird. Das liegt daran, dass die HTTPS-Verbindung des Cloud Connectors mit einem *selbstsignierten Zertifikat* (engl. Self-Signed Certificate) verschlüsselt wird. Dieses Zertifikat wird erstellt, wenn der Cloud Connector zum ersten Mal gestartet wird. In Kapitel 9, »Sichere Konfiguration«, erfahren Sie, wie Sie dieses UI-Zertifikat austauschen können. Wie in Abbildung 3.12 dargestellt, werden Sie auch darüber informiert, dass die Cloud-Connector-Instanz weder die Master- noch die Shadow-Rolle hat. Dies bedeutet, dass es sich um eine Installation handelt, die noch nicht konfiguriert wurde.

Abbildung 3.12 Cloud-Connector-Anmeldung

In der Standardkonfiguration speichert der Cloud Connector den Benutzer mit dem zugehörigen Passwort als Hash-Wert im Dateisystem. Dies ist der *File User Store*. Dies geschieht in einer XML-Datei namens users.xml im config-Verzeichnis. Die XML-Datei ist in Listing 3.1 dargestellt.

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users xmlns=http://tomcat.apache.org/xml
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation=http://tomcat.apache.org/xml tomcat-users.xsd
version="1.0">
<role rolename="admin"/>
<group groupname="initial" roles=""/>
<user username="Administrator" password=
"280D44AB1E9F79B5CCE2DD4F58F5FE91F0FBACDAC9F7447DFFC318CEB79F2D02" groups=""
roles="admin"/></tomcat-users>
```

Listing 3.1 users.xml

Der Cloud Connector ist ohne die Integration eines *LDAP*-Servers nicht mehrbenutzerfähig. Die erste Anmeldung am Cloud Connector erfolgt mit dem Benutzernamen *Administrator* und dem Passwort *manage*. Beachten Sie die Groß- und Kleinschreibung des Benutzernamens. Nach erfolgreicher Erstanmeldung werden Sie aufgefordert, das Passwort des Benutzers zu ändern, wie in Abbildung 3.13 dargestellt. Darüber hinaus müssen Sie angeben, ob der Administrator die Master- oder die Shadow-Instanz konfigurieren soll. Für den Dateibenutzerspeicher ist keine Kennwortrichtlinie festgelegt, aber dennoch sollten Sie ein komplexes Kennwort vergeben.

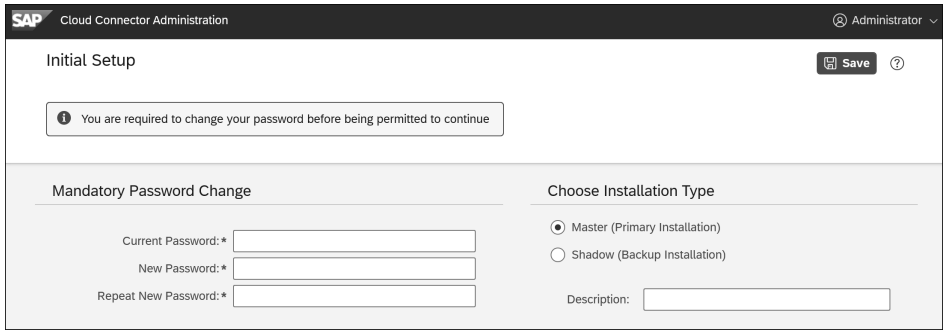


Abbildung 3.13 Erstmalige Anmeldung

Fehlerbehebung bei einem vergessenen Passwort

Es gibt keine direkte Möglichkeit, ein Kennwort mithilfe von Skripten in der Befehlszeile zu ändern. Wenn Sie jedoch das Kennwort für einen Benutzernamen vergessen

haben, gibt es eine Lösung. Diese ist in SAP-Hinweis 2388242 beschrieben und wie folgt kurz zusammengefasst:

1. Stoppen Sie den Cloud Connector.
2. Laden Sie eine portable Version des Cloud Connectors auf Ihren lokalen Computer herunter, und entpacken Sie sie.
3. Kopieren Sie aus der portablen Version die Datei users.xml aus dem config-Verzeichnis in das config-Verzeichnis Ihrer Cloud-Connector-Installation und überschreiben Sie die vorhandene Datei.
4. Starten Sie den Cloud Connector.
5. Melden Sie sich mit den Standardanmeldedaten an (Benutzername *Administrator* und Passwort *manage*).

Nachdem Sie das Passwort geändert haben, werden Sie zum Bereich **Define Subaccount** weitergeleitet, wie in Abbildung 3.14 dargestellt. Dort haben Sie die Möglichkeit, sich mit einem Subaccount von SAP BTP zu verbinden und einen HTTPS-Proxy zu definieren. Obwohl der Cloud Connector nur in Verbindung mit einem Subaccount sinnvoll ist, müssen Sie sich an dieser Stelle nicht mit einem Subaccount verbinden und können die Konfiguration auch schon vorher vornehmen.

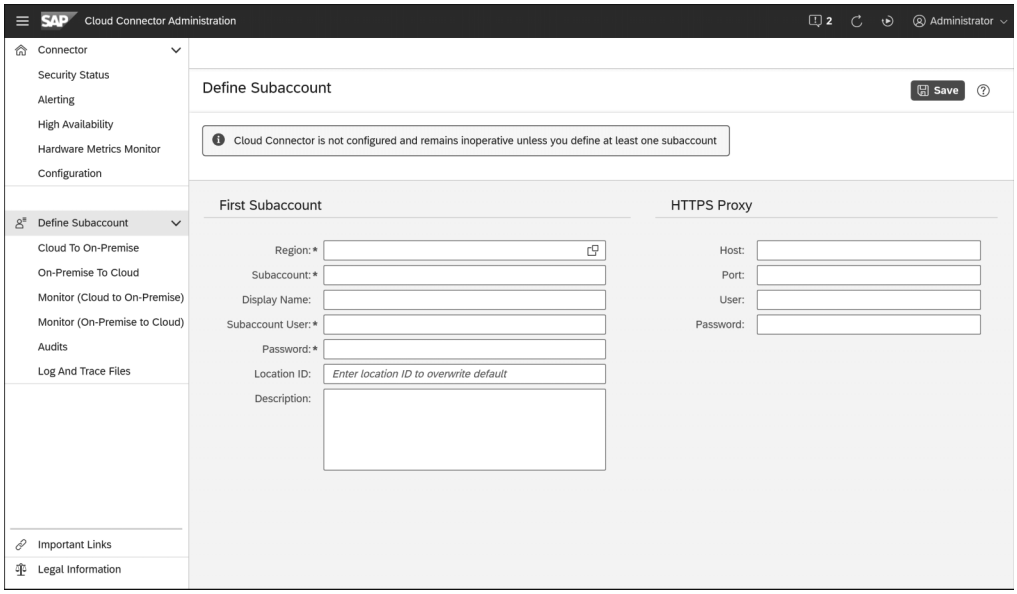


Abbildung 3.14 Verbindung zum SAP-BTP-Subaccount

Sie können die Konfiguration des Cloud Connectors über das Menü **Connector • Configuration** aufrufen. Die Konfiguration ist in die folgenden Bereiche unterteilt, wie in Abbildung 3.15 dargestellt:

- **User Interface**
- **Cloud**
- **On Premise**
- **Reporting**
- **Advanced**

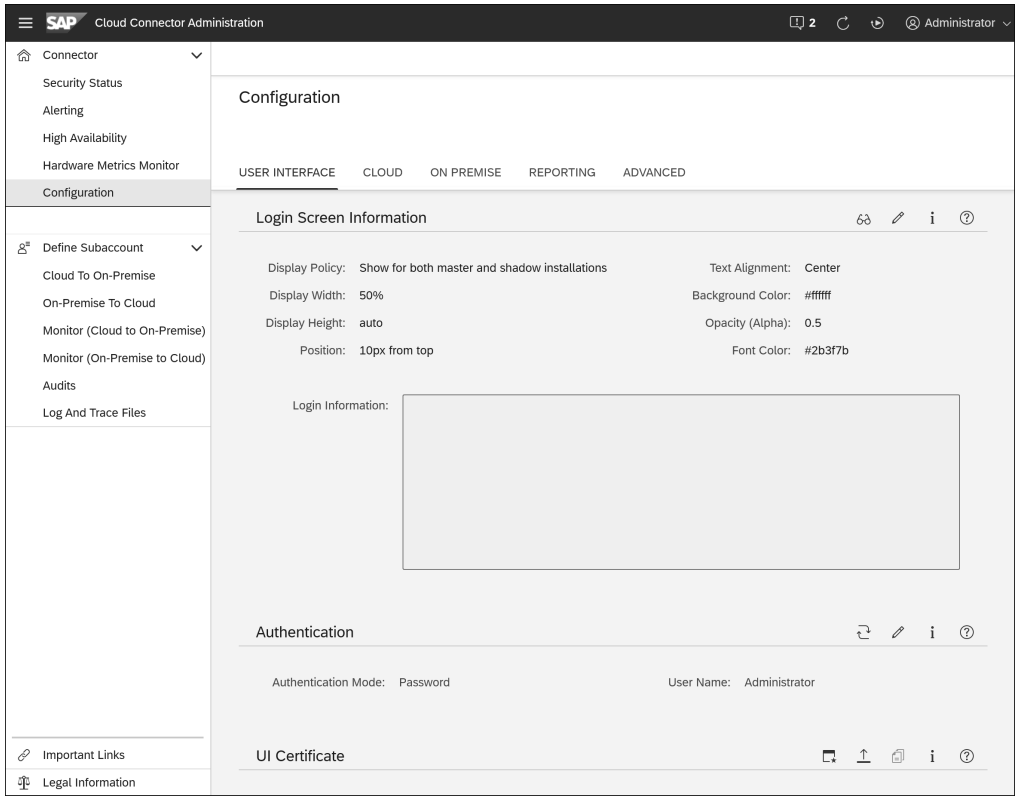


Abbildung 3.15 Grundlegende Konfiguration des Cloud Connectors

3.4.2 Konfiguration der Benutzeroberfläche

Im Abschnitt **User Interface** haben Sie die Möglichkeit, die auf dem Anmeldebildschirm angezeigten Informationen anzupassen. Klicken Sie dazu auf das Symbol . Sie können dann Anpassungen vornehmen, wie in Abbildung 3.16 dargestellt. Die Anmeldeinformationen werden in einem Kasten mit abgerundeten Ecken angezeigt. Über den Bereich **Display Policy** können Sie steuern, ob die Informationen in der Master-Instanz, der Shadow-Instanz, in beiden Instanzen oder gar nicht angezeigt werden. Sie können diese Option verwenden, um dem Benutzer mitzuteilen, ob er sich auf einem Entwicklungssystem, einem Testsystem oder dem Produktionssystem be-

findet. An dieser Stelle haben Sie die Möglichkeit, HTML zu verwenden. Die Verwendung unterliegt jedoch einigen Einschränkungen, die Sie in der Dokumentation des Cloud Connectors nachlesen können. Diese Einschränkungen beschränken sich hauptsächlich auf die Verwendung von Überschriften und Listenelementen.

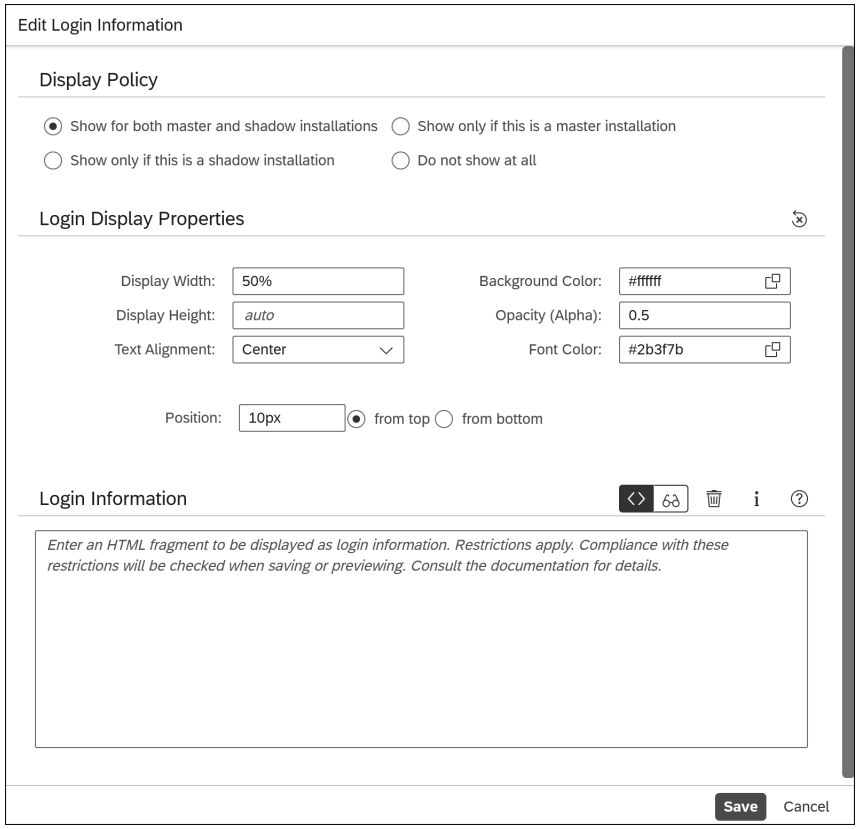


Abbildung 3.16 Anmeldeinformationen anpassen

Im Bereich **Authentication** können Sie die LDAP-Konfiguration vornehmen. Dies wird in Kapitel 9, »Sichere Konfiguration«, besprochen. Sie haben jedoch auch die Möglichkeit, die Anmeldedaten zu ändern (siehe Abbildung 3.17). Klicken Sie dazu auf das Symbol .

An dieser Stelle können Sie auch den Benutzernamen über das Feld **User Name** ändern. Um das Kennwort zu ändern, müssen Sie das aktuelle Kennwort des Benutzers in das Feld **Current Password** eingeben, dann ein neues Kennwort in das Feld **New Password** eingeben und es im Feld **Repeat New Password** wiederholen (siehe Abbildung 3.18).

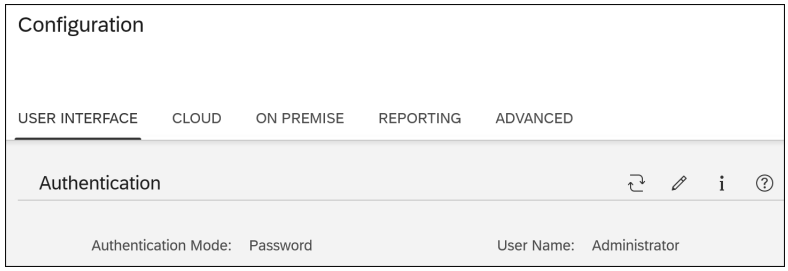


Abbildung 3.17 Konfiguration der Authentifizierung

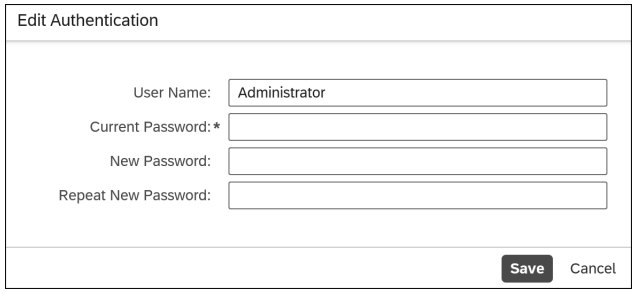


Abbildung 3.18 Authentifizierung bearbeiten

Im Bereich **Configuration** können Sie auch das UI-Zertifikat importieren (siehe Abbildung 3.19).

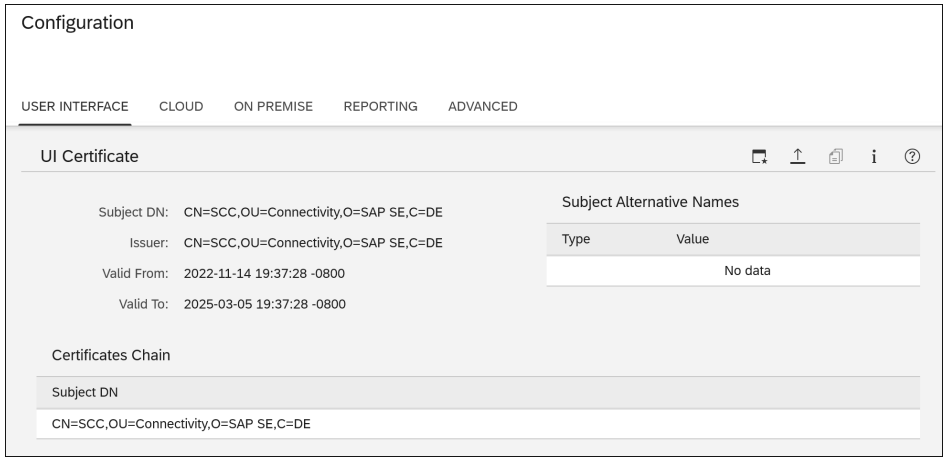


Abbildung 3.19 UI-Zertifikat

Der Cloud Connector wird mit einer Vielzahl von *Cipher Suites* geliefert, die ebenfalls in diesem Abschnitt zu finden sind (siehe Abbildung 3.20).

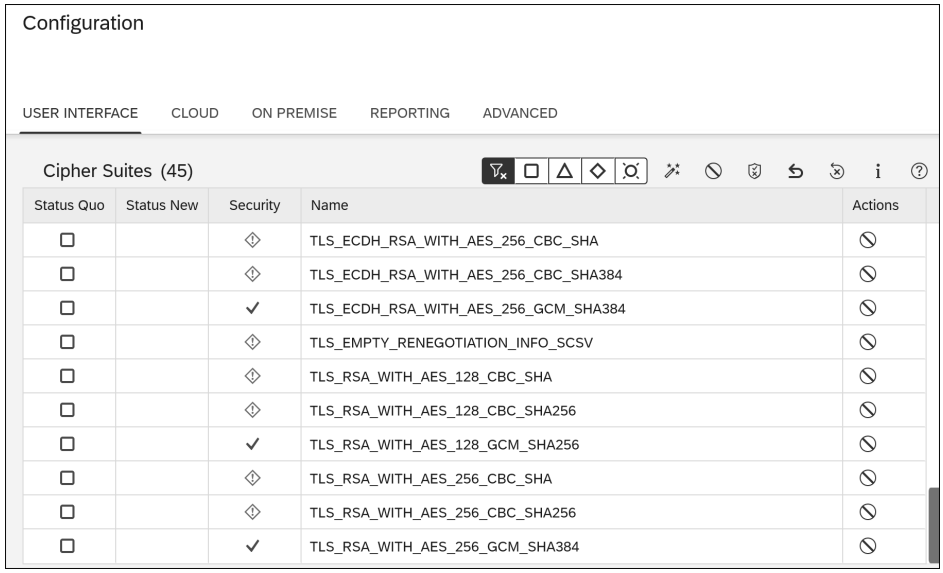


Abbildung 3.20 Cipher Suites

3.4.3 Cloud-Konfiguration

Im Bereich **Connector Info** auf der Registerkarte **Cloud** können Sie die Beschreibung des Cloud Connectors ändern, der bei der ersten Anmeldung zugewiesen wurde (siehe Abbildung 3.21).

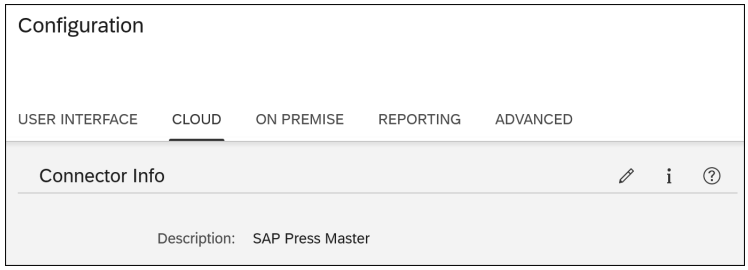


Abbildung 3.21 Connector-Info

Im Bereich **HTTPS Proxy** können Sie optional einen HTTPS-Proxy definieren. Dieser wird vom Cloud Connector verwendet, um den TLS-Tunnel zu den SAP-BTP-Subaccounts aufzubauen (siehe Abbildung 3.22).

Für den Proxy kann eine Kombination aus Host und Port gespeichert werden. Außerdem kann der von Ihnen verwendete Proxy eine Benutzerauthentifizierung erfordern. In diesem Fall können Sie auch einen Benutzernamen und ein zugehöriges Passwort hinterlegen (siehe Abbildung 3.23). Ein Verbindungstest mit dem Proxy wird derzeit vom Cloud Connector nicht unterstützt.

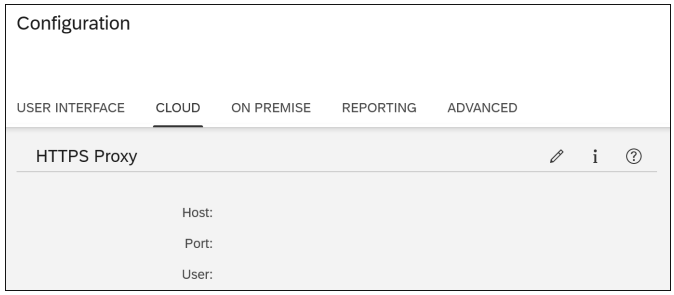


Abbildung 3.22 HTTPS-Proxy

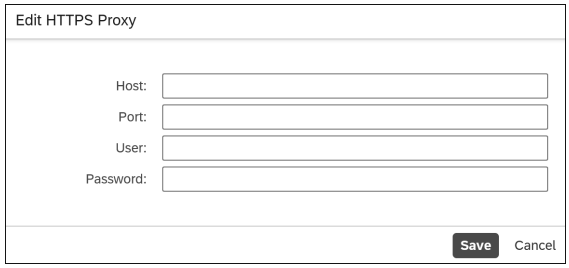


Abbildung 3.23 Proxy-Authentifizierung

Im Bereich **Cloud User Store** können Sie einen Cloud User Store konfigurieren (siehe Abbildung 3.24). Sie können Ihre SAP-BTP-Anwendungen so konfigurieren, dass sie den unternehmenseigenen LDAP-Server als Benutzerspeicher verwenden. In diesem Fall muss die Plattform nicht die gesamte Benutzerdatenbank pflegen, sondern fordert die erforderlichen Informationen aus dem unternehmenseigenen Benutzerspeicher an. Java-Anwendungen, die auf SAP BTP laufen, können diese Verbindung nutzen, um Anmeldedaten zu prüfen, nach Benutzern zu suchen und Details abzurufen. Zusätzlich zu den Benutzerinformationen kann die Cloud-Anwendung auch Informationen über die Gruppen abfragen, denen ein Benutzer in LDAP angehört. Daraus lassen sich in SAP-BTP-Berechtigungen ableiten.

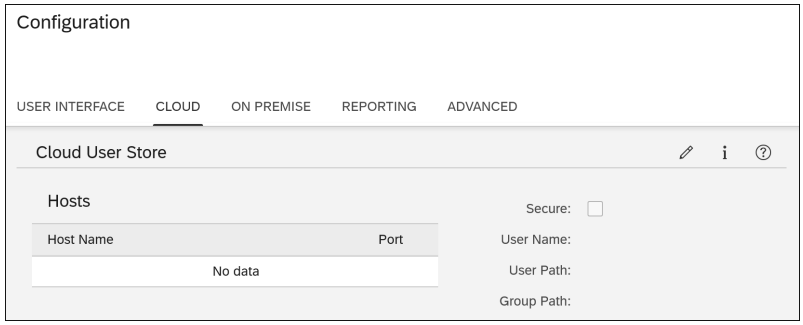


Abbildung 3.24 Cloud User Store

Für die Konfiguration müssen Sie Angaben für **Host Name** und **Port** machen, wie in Abbildung 3.25 dargestellt.

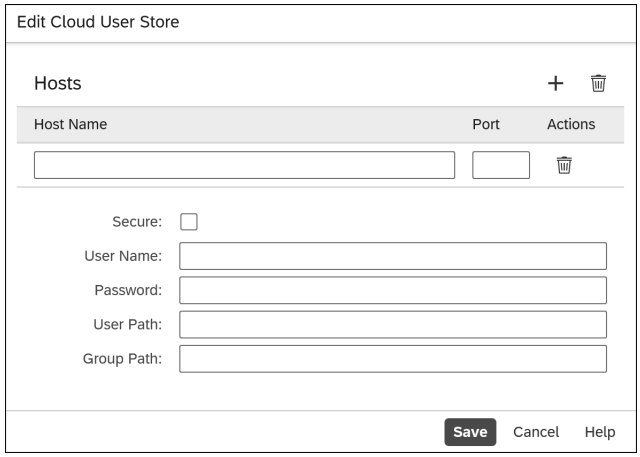


Abbildung 3.25 Konfiguration des Cloud User Store

Mit dem Kontrollkästchen **Secure** können Sie festlegen, ob LDAP over SSL/TLS (LDAPS) als Kommunikationsprotokoll verwendet werden soll. LDAPS ist eine sichere Version von LDAP, bei der die Übertragung von Daten zwischen Client und Server über eine sichere SSL/TLS-Verbindung verschlüsselt wird. Dadurch wird sichergestellt, dass die über das Netz übertragenen Daten vor unbefugtem Zugriff oder Manipulation geschützt sind. LDAPS ist besonders wichtig in sensiblen Netzwerken, in denen vertrauliche Informationen gespeichert werden. Das Attribut **User Name** enthält den Namen des technischen Benutzers, mit dem die Verbindung zum LDAP-Server hergestellt wird, und das Attribut **Password** enthält das zugehörige Passwort. Über das Attribut **User Path** können Sie den LDAP-Teilbaum konfigurieren, der die Benutzer enthält. Über das Attribut **Group Path** können Sie den LDAP-Teilbaum konfigurieren, der die Gruppen enthält.

Im Abschnitt **Custom Regions** können Sie Regionen hinzufügen, die in der Standardauswahl nicht verfügbar sind (siehe Abbildung 3.26).

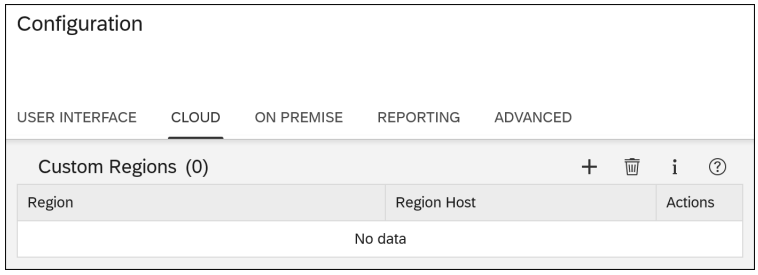


Abbildung 3.26 Custom Regions

Dies ist besonders nützlich für Regionen, die nach der Veröffentlichung Ihrer aktuellen Cloud-Connector-Version eingeführt wurden. Diese Regionen sind nicht in der Liste der vordefinierten Regionen enthalten.

3.4.4 On-Premise-Konfiguration

Um eine gegenseitige Authentifizierung zwischen dem Cloud Connector und jedem Backend-System, mit dem er sich verbindet, einzurichten, können Sie ein X.509-Client-Zertifikat in den Cloud Connector importieren (siehe Abbildung 3.27). Navigieren Sie dazu zur Registerkarte **On Premise** und zum Abschnitt **System Certificate**. Der Cloud Connector verwendet dann das Systemzertifikat für alle HTTPS-Anforderungen an Backends, die ein Client-Zertifikat erfordern. Die Zertifizierungsstelle (engl. Certificate Authority, CA), die das Client-Zertifikat des Cloud Connectors signiert hat, muss von allen Backend-Systemen, mit denen sich der Cloud Connector verbinden soll, als vertrauenswürdig eingestuft werden. An dieser Stelle gibt es auch eine Besonderheit: Wenn Sie auf das Symbol klicken, können Sie das UI-Zertifikat als Systemzertifikat übernehmen.

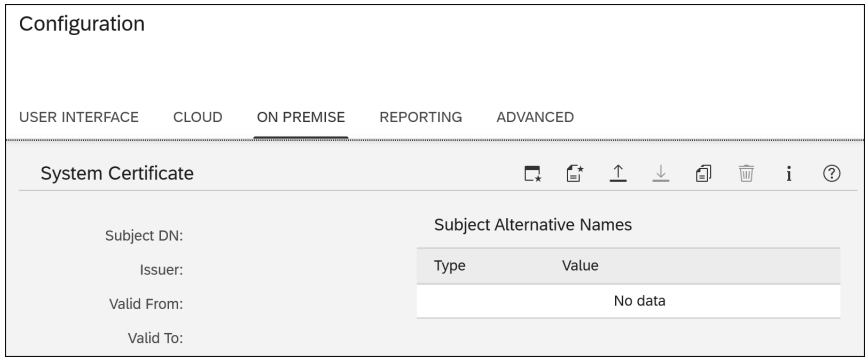


Abbildung 3.27 Systemzertifikat

Standardmäßig vertraut der Cloud Connector jedem lokalen System, wenn es sich über TLS mit ihm verbindet. Da dieses Verhalten aus Sicherheitsgründen unerwünscht sein kann, können Sie einen Trust Store konfigurieren, der als Liste vertrauenswürdiger Zertifizierungsstellen fungiert. Jedes TLS-Serverzertifikat, das von einer dieser Zertifizierungsstellen ausgestellt wurde, gilt als vertrauenswürdig. Wenn die Zertifizierungsstelle, die ein bestimmtes Serverzertifikat ausgestellt hat, nicht im Trust Store enthalten ist, gilt der Server als nicht vertrauenswürdig, und die Verbindung schlägt fehl. Navigieren Sie zum Abschnitt **Trust Store**, um die erforderliche Konfiguration vorzunehmen (siehe Abbildung 3.28).

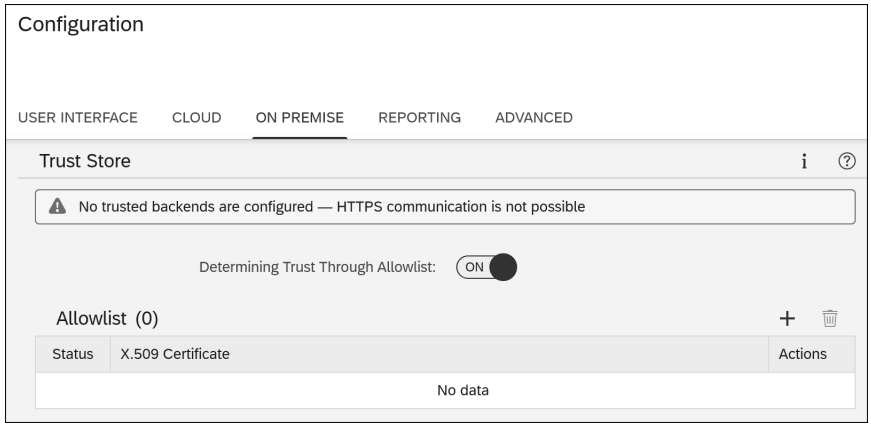


Abbildung 3.28 Trust Store

Der Cloud Connector verwendet den konfigurierten CA -Ansatz, um kurzlebige Zertifikate für die Registrierung mit derselben Identität im Backend auszustellen, die in der Cloud registriert ist. Um eine Trust-Beziehung mit dem Backend aufzubauen, sind die entsprechenden Konfigurationsschritte unabhängig vom Ansatz, den Sie für die CA wählen (siehe Abbildung 3.29).

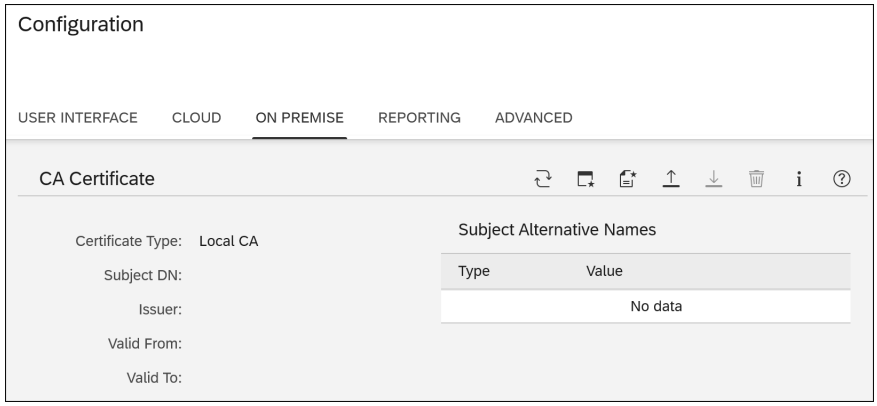


Abbildung 3.29 CA Certificate

Der Cloud Connector unterstützt Principal Propagation. In diesem Fall wird die Benutzeridentität von der Cloud-Anwendung an das Backend-System weitergegeben. Die erforderliche Konfiguration erfolgt im Bereich **Principal Propagation** (siehe Abbildung 3.30). Die Konfiguration der Principal Propagation wird in Kapitel 12, »Principal Propagation«, ausführlich erläutert.

Der Cloud Connector ermöglicht es Ihnen, in SAP BTP über Kerberos authentifizierte Benutzer gegen Backend-Systeme zu propagieren. Er verwendet die Kerberos-Protokollerweiterungen »Service for User« und »Constrained Delegation«. Bei diesem An-

satz wird das *Key Distribution Center* (KDC) zum Austausch von Nachrichten verwendet, um Kerberos-Token für einen bestimmten Benutzer und ein bestimmtes Backend-System abzurufen. Diese Funktion wird für ABAP-Backend-Systeme nicht unterstützt. In diesem Fall können Sie die zertifikatsbasierte Principal Propagation verwenden. Die erforderliche Konfiguration kann im Abschnitt **Kerberos** eingestellt werden (siehe Abbildung 3.31).

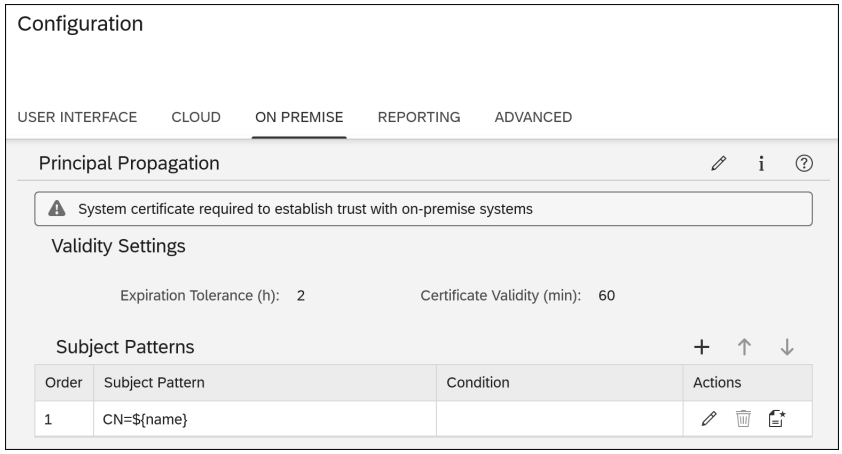


Abbildung 3.30 Principal Propagation

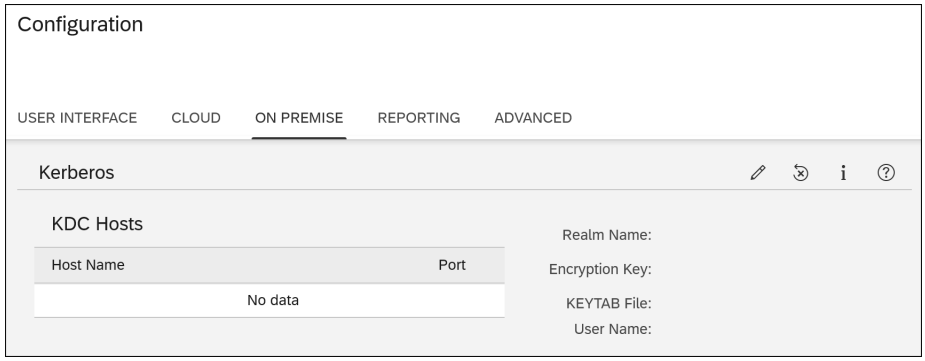


Abbildung 3.31 Kerberos konfigurieren

Der Cloud Connector ermöglicht es, Backend-Systeme über das bewährte RFC-Protokoll anzusprechen. Für eine reine RFC-Verbindung ist keine zusätzliche Konfiguration erforderlich. Wenn Sie jedoch eine sichere Netzwerkverbindung auf Basis von *Secure Network Communications* (SNC) verwenden wollen, müssen Sie die erforderliche Konfiguration im **SNC**-Bereich vornehmen (siehe Abbildung 3.32). Als Voraussetzung müssen Sie eine SNC-Bibliothek installieren. Die Konfiguration von SNC wird in Kapitel 9, »Sichere Konfiguration«, ausführlich beschrieben.

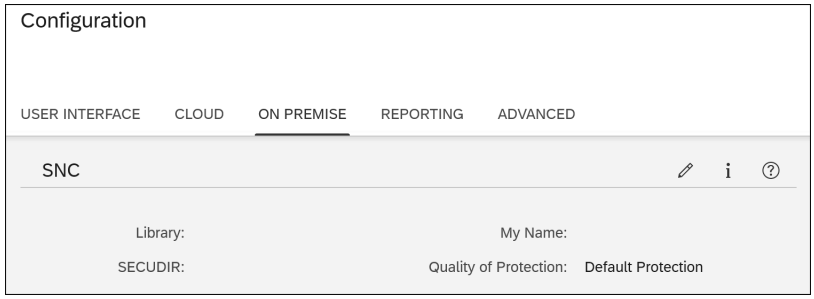


Abbildung 3.32 SNC

SNC ist eine Funktionalität in SAP-Systemen, die eine sichere Übertragung von Daten ermöglicht. Mit SNC kann die Kommunikation zwischen verschiedenen SAP-Systemen und -Komponenten über eine sichere Verbindung erfolgen, die vor Manipulation und Überwachung geschützt ist. SNC ist ein wichtiger Bestandteil von SAP-Lösungen für Sicherheit und Compliance, insbesondere im Hinblick auf die Übertragung sensibler Daten. Der Einsatz von SNC trägt dazu bei, dass Unternehmen ihre Datensicherheit gewährleisten und Vorschriften und Gesetze einhalten können.

3.4.5 Reporting-Konfiguration

Wenn Sie den Cloud Connector mit dem SAP Solution Manager überwachen möchten, müssen Sie einen Host-Agenten auf dem Cloud-Connector-Rechner installieren und den Cloud Connector auf Ihrem System registrieren. Sie müssen die erforderliche Konfiguration im Bereich **Solution Manager** auf der Registerkarte **Reporting** vornehmen (siehe Abbildung 3.33). Die erforderliche Konfiguration ist in SAP-Hinweis 2607632 beschrieben.

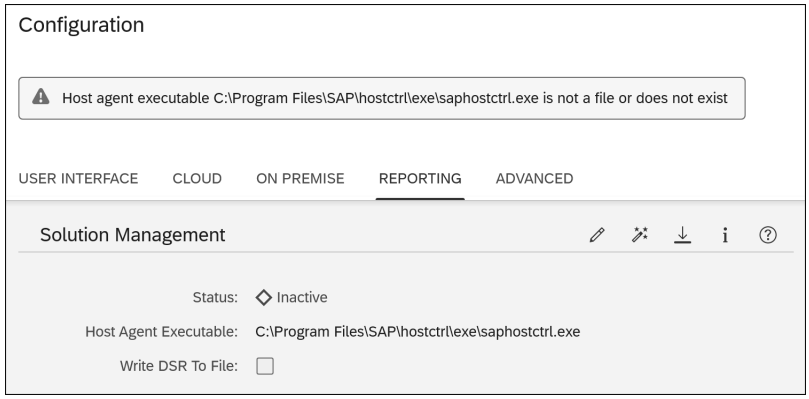


Abbildung 3.33 SAP-Solution-Manager-Integration

3.4.6 Advanced-Konfiguration

Im Abschnitt **Connectivity** auf der Registerkarte **Advanced** haben Sie die Möglichkeit, die Verbindungseinstellungen anzupassen. Dies steuert den Durchsatz und die HTTP-Verbindung zu On-Premise-Systemen (siehe Abbildung 3.34) wie folgt:

- **Application Tunnel Connections**
  Dieser Parameter gibt den Standardwert für die maximale Anzahl von Tunnelverbindungen pro Anwendung an.
- **Tunnel Worker Threads**
  Dieser Parameter steuert die Anzahl der Worker-Threads, die für alle Anfragen verwendet werden.
- **Protocol Processor Worker Threads**
  Dieser Parameter steuert die Anzahl der Worker-Threads, die für die Protokollverarbeitung verwendet werden.
- **Max. Reconnect Attempts**
  Dieser Parameter steuert die maximale Anzahl der Wiederverbindungsversuche.
- **Max. Chunk Size HTTP Packages (kb)**
  Dieser Parameter steuert die maximale Größe der beim HTTP-Streaming übertragenen Chunks. Die Chunk-Größe beeinflusst den Durchsatz der HTTP-Kommunikation.
- **Max. HTTP Request Header Length (kb)**
  Dieser Parameter steuert die maximal zulässige Größe der HTTP-Anfrage-Header. Header, die Authentifizierungsinformationen wie SAML oder ein JSON Web Token (JWT) enthalten, können diese Größe erfordern. JWT ist ein Standardformat für die Übertragung von Benutzerauthentifizierungsinformationen zwischen Parteien über das Internet.
- **Max. Size HTTP Request (kb)**
  Dieser Parameter steuert die Größe der Anfragezeile einer HTTP-Anfrage. Der HTTP-Body ist nicht enthalten.
- **Max. HTTP Response Header Length (kb)**
  Dieser Parameter steuert die maximal zulässige Größe von HTTP-Antwort-Headern.
- **Max. Size HTTP Response (kb)**
  Dieser Parameter steuert die Größe der Antwortzeile der HTTP-Antwort. Der HTTP-Body ist nicht enthalten.

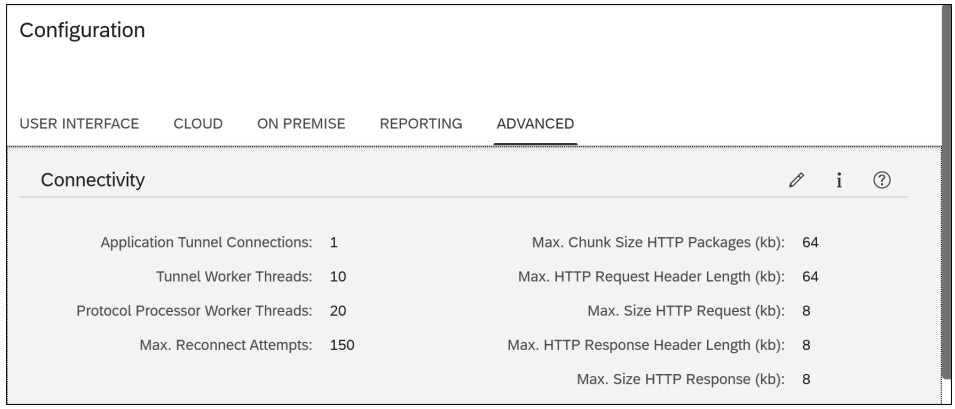


Abbildung 3.34 Konfiguration der Connectivity

Im Bereich **JVM** haben Sie die Möglichkeit, die JVM-Einstellungen anzupassen, die die Speicherverwaltung steuern (siehe Abbildung 3.35). Ein Neustart ist erforderlich, wenn die JVM-Einstellungen geändert werden. Die folgenden Parameter können konfiguriert werden:

- **Initial Heap Size**
- **Maximal Heap Size**
- **Maximal Direct Memory**

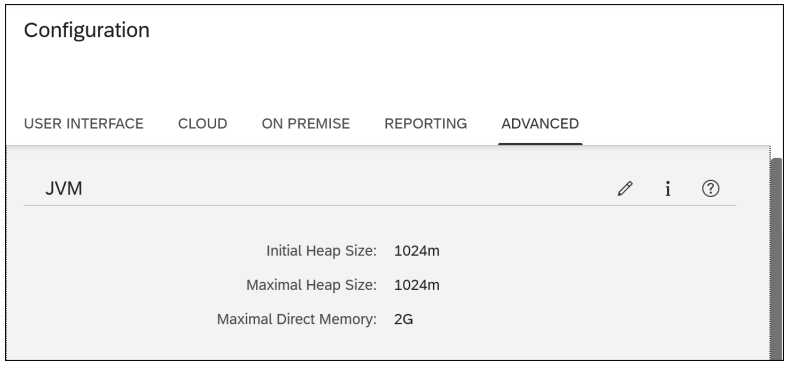


Abbildung 3.35 JVM-Einstellungen

Diese Parameter wurden in Abschnitt 3.1 ausführlich erläutert. Wenn Sie den Cloud Connector entsprechend Ihren Anforderungen dimensionieren, müssen Sie die Einstellungen an dieser Stelle anpassen.