SAP HANA Cloud Connector – Solution Brief

Applies to:

SAP HANA Cloud Connector, SAP HANA Cloud Platform

Summary

This document is a solution brief about the SAP HANA Cloud connector, the secure and reliable on-demand to on-premise connectivity solution of the SAP HANA Cloud Platform.

SAP SE, December 2014

Table of Contents

Connectivity Made Easy with SAP HANA Cloud Connector

Introduction

The SAP HANA Cloud Platform (shortly, HCP) is a Platform-as-a-Service (shortly, PaaS) offering that enables developers to build, extend, and run applications in the cloud. It is the industry's only in-memory cloud platform powered by the SAP HANA database. It provides developers a set of application and database services and features native HANA and open Java developer experiences.

HCP provides out-of-the-box connectivity to customers' on-premise landscapes which allows easy and secure integration of cloud applications with systems running in protected customer networks. This enables hybrid scenarios and allows customers to innovate in areas like mobile, social or big data using SAP's HCP platform. By this, customers can save investments made in their on-premise IT assets, while taking advantage of cloud benefits at the same time, such as low TCO, faster development cycles or rapid ramp-up time, and thus save time, cost and complexity compared to conventional integration products.

Target audience

- CTOs
- System and IT administrators
- Solution architects

This document does not replace the HCP documentation [1], documentation of the Cloud Connector [2], the Cloud Connector's operator's guide [3] or its security whitepaper [4].

Solution Overview

The SAP HANA Cloud Connector (shortly, Cloud Connector) enables hybrid scenarios in which cloud applications access and extend on-premise systems, or on-premise database tools connect to HANA databases on SAP HANA Cloud Platform. It establishes secure technical connectivity between HCP accounts and a protected on-premise network, and can be combined with higher-level SAP integration solutions, like SAP HANA Cloud Integration for process integration.

The Cloud Connector thereby acts as an integration component running in the on-premise network that is able to establish secure and reliable connectivity from the on-premise network to accounts on HCP, each connected HCP account requiring separate authentication and coming with an own set of configuration. Once connectivity is established, applications running in the related HCP account are able to access on-premise systems which have been configured as accessible resources in the Cloud Connector. An arbitrary number of SAP and non-SAP on-premise systems can be used with a single Cloud Connector instance, and it is not necessary to touch an on-premise system in order to use it in combination with the Cloud Connector, unless trust shall be configured between the Cloud Connector and the system (this is needed for principal propagation, for instance).

The Cloud Connector provides administration and monitoring capabilities, like fine-grained access control of the on-premise resources exposed to the cloud, a whitelisting of cloud applications which are authorized to use the Cloud Connector at all, an auditing service, usage of a corporate LDAP for authentication of the Cloud Connector administration UI, and others. The Cloud connector can be optionally operated in a high availability mode in which a second redundant so-called *shadow Cloud Connector* is installed which takes over from the master instance once it becomes unavailable. The Cloud Connector also takes care to automatically re-establish connections in case they break due to temporary network issues.

The Cloud Connector can also be used to connect on-premise database tools via JDBC/ODBC connections to databases running on HCP. The database traffic is then forwarded through the encrypted tunnel of the Cloud Connector to the target database in the cloud.

For inbound communication, the Cloud Connector supports HTTP and RFC as protocols, and JDBC/ODBC access for outbound connectivity. Java and XS applications running on HCP can use arbitrary REST- or SOAP-APIs to call on-premise Web Services through the Cloud Connector. Java applications can additionally use SAP Java Connector API (a.k.a. JCo) for direct access of on-premise ABAP systems.

The Cloud Connector also supports principal propagation, i.e. a reliable forwarding of the user identify of the cloud user to an on-premise system. This is often needed for scenarios where the identity of the end user must be propagated to the on-premise system in order to do reasonable actions, like for instance booking vacation for an employee in a leave request application running in the cloud that is connected to an on-premise ERP system.

Figure 1 shows how the landscape looks like if the Cloud Connector is used for secure connectivity between HCP applications and on-premise networks.

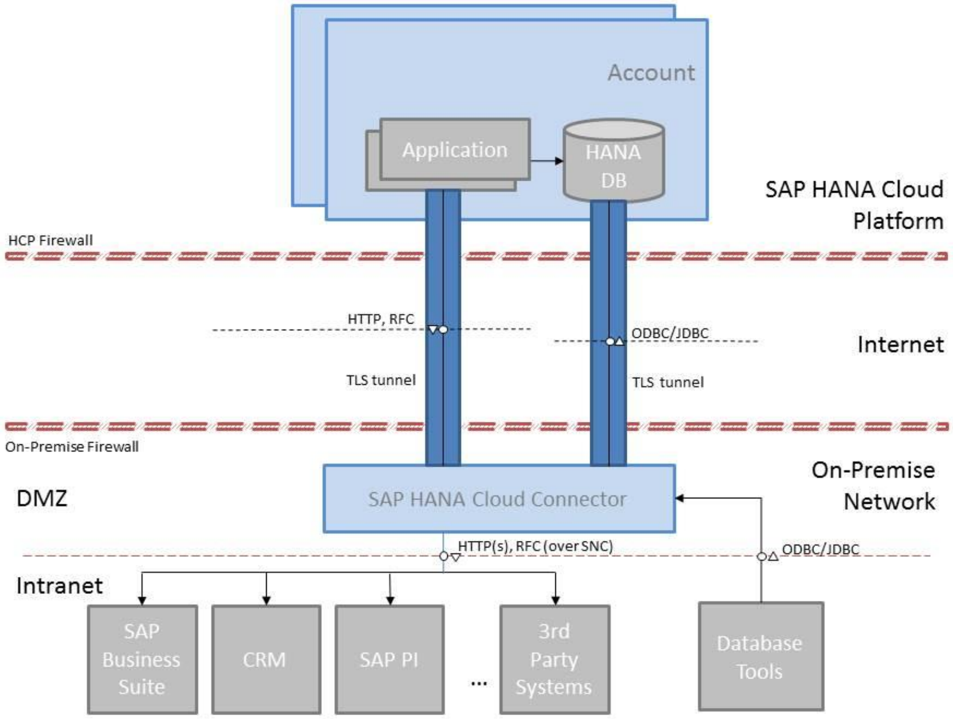

Figure 1 Typical cloud/on-premise connectivity landscape using SAP HANA Cloud Platform and the Cloud Connector

Security

Security is one of the major topics considered by the Cloud Connector. Following core principles have been taken into account from day one of its development:

- Ability to keep on-premise firewalls closed to inbound traffic:
  It should not be necessary to open firewall ports for inbound traffic to an on-premise network in order to make on-premise resources accessible for HCP cloud applications. Open ports in a company’s firewall increase the attack vector and usually require complex audits and discussions with central IT departments before being approved. The Cloud Connector is able to establish the connection to HCP accounts by so-called *reverse invoke* approach, i.e. the connection is established from within the on-premise network to the cloud.
- Give full control over the connectivity to HCP into hands of on-premise IT staff:
  The IT staff on the on-premise side should have full control when to open or close connectivity via the Cloud Connector to HCP, to which HCP accounts to establish a connection, which systems and resources to expose to the connected HCP accounts, and which cloud applications to authorize to use the connectivity at all. There is no possibility to control and change those configurations from cloud side.
- End-to-end encryption between the Cloud Connector and HCP:
  The Cloud Connector takes care to encrypt all traffic sent over the connection, independent of the used protocols. The communication between the cloud application and the Cloud Connector is always TLS-encrypted so that confidentiality is guaranteed.

- Mutual authentication between Cloud Connector and connected HCP endpoints:
  To ensure that only trusted parties communicate with each other, mutual authentication between the Cloud Connector and connected HCP endpoints is performed when establishing new connections.
- Isolation of HCP accounts:
  The platform takes care of strong isolation of HCP accounts and their resources, so that it is impossible for applications of one account to use the connectivity to an on-premise network of a different account.

Further security details and guidelines can be found in the Cloud Connector security whitepaper.

Enterprise Ready for Business Applications

The Cloud Connector is designed for being used by business critical applications. It provides enterprise-grade features like high availability to ensure 24x7 availability of the connectivity between the related on-premise network and the cloud, or a reliable way to propagate a cloud user identity to connected on-premise systems. It allows authenticating trusted Cloud Connector instances towards security-critical on-premise systems by using X.509 certificates, and provides an audit log for which the integrity can be verified. The Cloud Connector is administrated by a Web UI for which a corporate LDAP system can be used to authenticate administrator users of Cloud Connector.

Ease of Use

Installation, upgrade and configuration of the Cloud Connector are easy tasks and can be done in minutes rather than hours. No big and cost intensive IT projects are needed to setup the landscape for hybrid scenarios and to establish secure connections to HCP. The Cloud Connector as well as HCP provide intuitive, easy to use administration UIs to setup and configure applications and its connectivity. This allows setting up and operating the Cloud Connector either centrally by an IT department, as well as by IT experts close to the line-of-business.

Scenarios

The Cloud Connector is built and recommended for following scenarios.

On-premise Extension Scenarios

In an on-premise extension scenario HCP applications extend existing on-premise applications or integrate with on-premise systems. By using the cloud for such extensions, a customer can benefit from typical cloud advantages like low TCO, faster innovation cycles and low risk of breaking running systems. The cloud connector serves as integration component for secure and reliable connectivity between HCP and the needed systems in the customer network. A typical landscape setup is shown in Figure 2 below.

A few examples for this scenario are:

- Web shop application running in the cloud that integrates with an on-premise business suite for triggering sales orders.
- Analysis and monitoring application in the cloud that analyzes real-time data on HANA and triggers alerts or maintenance requests in a connected on-premise CRM system when certain events happen.
- Employee or manager self-service applications which shall be accessible on mobile devices and outside of the company Intranet and integrate with on-premise ERP systems.

The Cloud Connector fits well for point-to-point integration scenarios in which cloud applications directly integrate with on-premise systems, as well as for more complex process integration scenarios, in which an Enterprise Service Bus, like HANA Cloud Integration for process integration, is used to orchestrate processes between business partners.

Compared to traditional reverse proxy approaches where on-premise resources are made available to an external application via special firewall and DMZ configurations, the Cloud Connector has several advantages:

- It does not require configuration and changes in a company’s firewall and exposure of service endpoints to the internet. Attacks from the internet, like DoS, are not possible and thus its connectivity is significantly more secure compared to a reverse proxy set ups.
- It supports the RFC protocol and allows direct access to ABAP systems from cloud applications.
- It allows propagation of the cloud user identity in a trusted manner to connected on-premise target systems.

- It is easy to set up and configure in minutes and does not require complex and expensive IT projects to be introduced. It can also be operated in the line-of-business.

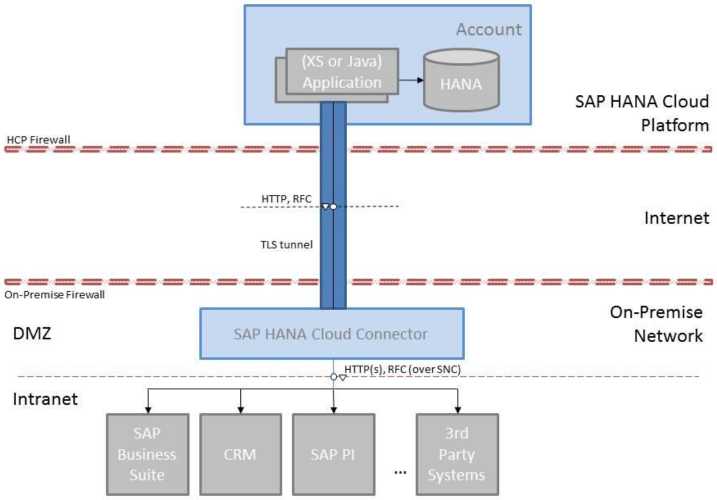

Figure 2 Typical landscape setup of an on-premise extension scenario

Connectivity to HANA Database in the Cloud

A second scenario for which the cloud connector can be used is to connect on-premise database tools to HANA databases in the cloud. With this, it is possible to use existing on-premise analysis tools, like SAP Business Objects Enterprise or Lumira, as well as replication and ETL tools, like SAP Landscape Transformer or SAP Data Services, in combination with HANA in the cloud. Figure 3 shows a typical landscape set up for this scenario.

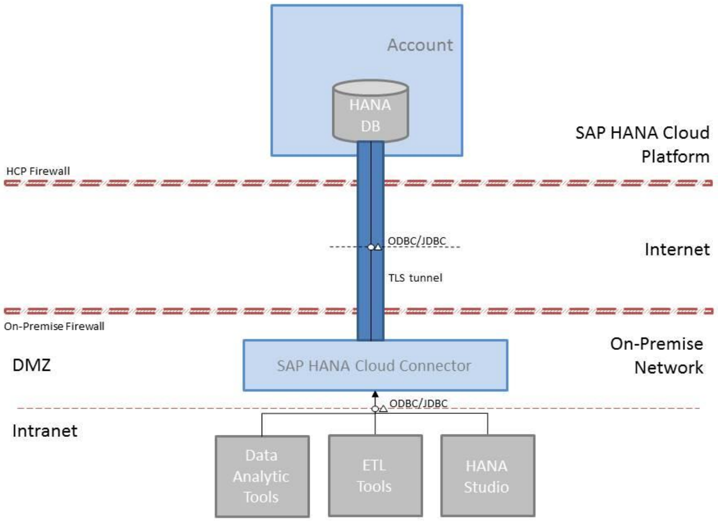

Figure 3 Typical landscape setup how to connect remote database tools with HANA on HCP

References

[1] SAP HANA Cloud Platform documentation
https://help.hana.ondemand.com/help/frameset.htm

[2] SAP HANA Cloud connector documentation
https://help.hana.ondemand.com/help/frameset.htm?e6c7616abb5710148cfcf3e75d96d596.html

[3] Operator's guide for SAP HANA Cloud connector
https://help.hana.ondemand.com/help/frameset.htm?2dded649c62c4fd8a65933f497042f14.html

Copyright

These materials are subject to change without notice. These materials are provided by SAP SE and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.