SAP HANA Cloud Connector - Security Whitepaper

Applies to:
SAP HANA Cloud Connector, SAP HANA Cloud Platform

Summary
This whitepaper provides an overview on the security concept of the SAP HANA Cloud Connector, which is the secure and reliable on-demand to on-premise connectivity solution of the SAP HANA Cloud Platform. It should answer questions of solution architects and IT administrators how integration of on-demand applications running on SAP HANA Cloud Platform with on-premise systems in protected networks are secured by the SAP HANA Cloud Connector.

SAP SE, December 2014
Table of Contents

Introduction ................................................................................................................................. 3
Target audience .......................................................................................................................... 3
The Physical and Environmental Layer ..................................................................................... 3
The Cloud Infrastructure Layer ................................................................................................. 4
The Service Layer: Cloud connector security at a glance .......................................................... 4
  Network Zones ......................................................................................................................... 5
  Inbound Connectivity ............................................................................................................... 5
  Outbound Connectivity .......................................................................................................... 6
Security Guidelines .................................................................................................................... 6
Introduction

Security is a crucial concern for any cloud-based solution and has major impact on the business decision of enterprises whether or not to make use of such solutions. SAP HANA Cloud Platform (shortly, HCP) is a platform-as-a-service offering designed to run business critical applications and processes for enterprises, with security considered on all levels of the on-demand platform. Figure 1 outlines the security relevant layers of the platform and provides some examples of security measures considered in the respective layer.

HCP provides the SAP HANA Cloud connector (shortly, Cloud Connector) to allow integrations of on-demand applications with services and systems running in secured customer networks, as well as to support secure database connections from the customer network to SAP HANA databases running on HCP. As these are highly security sensitive topics, this document gives an overview how the Cloud Connector ensures highest security standards for the mentioned scenarios.

Target audience

- System and IT administrators
- Technology consultants
- Solution architects

This document does not replace the HCP documentation, the documentation of the Cloud Connector, or the Cloud connector’s operator’s guide. It is also neither meant as manual nor as a getting started documentation for the Cloud Connector. A detailed introduction into HCP can be found in [1]. The Cloud Connector is documented in [2, 3], and its operator’s guide is available in [4].

The Physical and Environmental Layer

HCP runs in SAP-hosted data centers which are compliant with regulatory requirements as described in [5, 6]. To name two exemplary security measures, they consist of

- strict physical access control mechanisms using biometrics, video surveillance, and sensors;
- high availability and disaster recoverability with redundant power supply and own power generation
The Cloud Infrastructure Layer
HCP’s infrastructure and network facilities ensure security on network layer by granting access to the physical infrastructure of the platform and its applications only to authorized persons and only for a specific business purpose. The HCP landscape runs in an isolated network, which is protected from the outside by Firewalls, DMZ, and communication proxies for all inbound and outbound communications to and from the network.

The HCP infrastructure layer also ensures that platform services, like the connectivity service, and applications are running in isolation in sandboxed environments, and interaction between them is only possible over a secure remote communication channel.

The Service Layer: Cloud connector security at a glance
HCP’s Connectivity Service can be used to securely integrate on-demand applications with systems running in isolated customer networks. For this, the Cloud Connector needs to be installed as integration agent in the on-premise network and can then be used to establish a persistent SSL tunnel to HCP accounts. To establish this tunnel, the Cloud Connector Administrator has to authenticate himself against the related HCP account of which he must be member. Once the tunnel is established, it can be used by applications of the connected account to remotely call systems in the customer network.

Figure 2 shows an illustration of a system landscape in which the Cloud Connector is used for secure connectivity between HCP applications and on-premise systems. A single Cloud Connector instance can be connected to multiple HCP accounts, each connection requiring separate authentication and defining an own set of configuration. An arbitrary number of SAP and non-SAP systems can be connected to a single Cloud Connector instance. The on-premise system does not need to be touched to use it in combination with the Cloud Connector, unless trust shall be configured between the Cloud Connector and the on-premise system (this is needed for principal propagation, for instance). The Cloud Connector can also be operated in a high availability mode. In this case, a second redundant so-called shadow Cloud Connector must be installed which takes over from the master instance in case it becomes unavailable.

The Cloud Connector also supports the communication direction from the on-premise network to the HCP account with the so-called database tunnel. This allows the connection of common ODBC/JDBC database tools to SAP HANA databases and other provided databases in HCP.
Network Zones

A company network is usually divided into multiple network zones according to the security level of the contained systems. The DMZ network zone usually contains and exposes the external-facing services of an organization to an untrusted network, usually the Internet. Besides this, there are usually one or multiple other network zones which contain the components and services provided in the company’s intranet.

The Cloud Connector can be set up either in the DMZ or in an inner network zone. Technical prerequisites for the Cloud Connector to work properly are:

- The Cloud Connector must have access to the SAP HANA Cloud Platform landscape host, either directly or via HTTPS proxy (see [10]).
- The Cloud Connector must have direct access to the internal systems it shall provide access to. I.e. there must be transparent connectivity between the Cloud Connector and the internal system.

It’s a company’s decision, whether the Cloud Connector is set-up in the DMZ and operated centrally by an IT department or set-up in the intranet and operated by the line-of-business.

Inbound Connectivity

For inbound connections into the on-premise network, the Cloud Connector acts as a reverse invoke proxy between HCP and the internal systems. It is important to notice that once installed, none of the internal systems are accessible by default through the Cloud Connector: each system and on every system each service and resource which shall be exposed to HCP must be configured explicitly in the Cloud Connector. The Cloud Connector administrator also has the possibility to specify a virtual host name and port for a configured on-premise system, which is then used in the cloud. By this, it can be avoided that information on physical hosts is exposed to the cloud.

The SSL tunnel is established from the Cloud Connector to HCP via so-called reverse invoke approach. This gives full control of the tunnel into the hands of the Cloud Connector administrator, i.e. the tunnel can’t be established from the cloud or from somewhere else outside the company network, and the Cloud Connector administrator is the one who decides when the tunnel is established or closed.

The tunnel itself is using TLS (Transport Layer Security) with strong encryption of the communication, and mutual authentication of both sides of the communication, the client-side (Cloud Connector side) and the server-side (HCP cloud). The X.509 certificates which are used to authenticate the Cloud Connector and the HCP account are issued and controlled by HCP and kept in secure storages in the Cloud Connector and the cloud. Having the tunnel encrypted and authenticated, confidentiality and authenticity of the communication between the HCP applications and the Cloud connector is guaranteed.

As additional level of control, the Cloud Connector optionally allows restricting the list of HCP applications which are able to use the tunnel at all. This is useful in situations where multiple applications are deployed in a single HCP account while only particular applications should require connectivity to on-premise systems.

HCP guarantees strict isolation on account level by measurements on its infrastructure and platform layer, meaning that an application of one account is not able to access and use resources of another account. For the connectivity service, this means that an HCP application of one account can’t access the tunnel of another account.

The Cloud Connector supports inbound connectivity for HTTP and RFC, any other protocol is not supported. The payload sent via these protocols is encrypted on TLS/tunnel-level. For the route from the Cloud Connector to the on-premise systems, the Cloud Connector administrators have the choice for each configured on-premise system whether HTTP, HTTPS, RFC or RFC over SNC should be used. For HTTPS, a so-called system certificate can be configured in the Cloud Connector which is used for the trust relationship between the Cloud Connector and the connected on-premise systems. For RFC over SNC an SNC PSE can be configured in the Cloud Connector respectively.

The Cloud Connector also supports principal propagation of the cloud user identity to connected on-premise systems. For this, the system certificate (in case of HTTPS) or the SNC PSE (in case of RFC) is mandatory to be configured and trust with the respective on-premise system must be established. Trust configuration, in particular for principal propagation, is the only reason to configure and touch the used on-premise systems when using the Cloud Connector.

As audit logging is a critical element of an organization’s risk management strategy, the Cloud Connector provides audit logging for the complete record of access between cloud and Cloud Connector, as well as of configuration...
changes done in the Cloud Connector. The written audit log files are digitally signed by the Cloud Connector so that they can be checked for integrity, as described in [7].

The audit log data of the Cloud Connector can be used to alert Cloud Connector administrators regarding unusual or suspicious network and system behavior. Additionally, the audit log data can provide auditors with information required to validate security policy enforcement and proper segregation of duties. IT staff can use the audit log data for root-cause analysis following a security incident. Information how to configure and use the audit logging in the Cloud connector administrator UI can be found in [7].

Outbound Connectivity

The Cloud Connector also supports the communication direction from the on-premise network to HCP for the so-called database tunnel. It is used to connect local database tools via JDBC or ODBC to the SAP HANA DB or other databases on HCP, for instance SAP Business Objects tools like Lumira, BOE or Data Services.

The database tunnel only allows JDBC and ODBC connections from the Cloud Connector into the cloud; a reuse for other protocols is not possible. The tunnel uses the same security mechanisms as for the inbound connectivity, i.e. TLS-encryption and mutual authentication, as well as audit logging when and by whom a database tunnel has been established or closed.

The Cloud Connector can also be used solely for the purpose of the database tunnel – in this is the case there should be no inbound communication configured at all. Then only communication from the on-premise network to the HANA DB in the cloud would be allowed through the Cloud Connector.

To use the database tunnel, two different HCP users are needed: First, a platform user associated as member of the HCP account is needed to establish the database tunnel to the HANA DB, and second a HANA DB user is needed for the ODBC/JDBC connection to the database itself. For the HANA DB user, the role and privilege management of HANA can be used to control which actions the related user actually can perform on the database.

Security Guidelines

The following table lists security guidelines of SAP for a secure usage of the Cloud Connector.

<table>
<thead>
<tr>
<th>Security Measurement</th>
<th>Description</th>
<th>Recommendation</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network zone</td>
<td>Depending on the needs of the project, the Cloud Connector can be either set-up in the DMZ and operated centrally by the IT department or set-up in the intranet and operated by the line-of-business.</td>
<td>For access to highly secure on-premise systems, it is recommended to operate the Cloud Connector centrally by the IT department and to install it in the DMZ of the company network. It is also recommended to set up trust between the on-premise system and the Cloud Connector and to only accept requests from trusted Cloud Connectors in the system.</td>
<td>1</td>
</tr>
<tr>
<td>OS level protection of Cloud Connector machine</td>
<td>The Cloud Connector is a security critical component that handles the inbound access from HCP applications to systems of an on-premise network. Methods to harden the operating system on which the Cloud Connector is</td>
<td>Restrict the access to the operating system on which the Cloud Connector is installed to the minimal set of users who shall administrate the Cloud Connector. Use the machine which runs the Cloud Connector only for this purpose and</td>
<td>2</td>
</tr>
</tbody>
</table>

### Security Measurement

- **Network zone**: Depending on the needs of the project, the Cloud Connector can be either set-up in the DMZ and operated centrally by the IT department or set-up in the intranet and operated by the line-of-business.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>For access to highly secure on-premise systems, it is recommended to operate the Cloud Connector centrally by the IT department and to install it in the DMZ of the company network. It is also recommended to set up trust between the on-premise system and the Cloud Connector and to only accept requests from trusted Cloud Connectors in the system.</td>
<td>1</td>
</tr>
<tr>
<td>Restrict the access to the operating system on which the Cloud Connector is installed to the minimal set of users who shall administrate the Cloud Connector. Use the machine which runs the Cloud Connector only for this purpose and</td>
<td>2</td>
</tr>
</tbody>
</table>

---

SAP COMMUNITY NETWORK

© 2014 SAP SE

scn.sap.com
<table>
<thead>
<tr>
<th>Protection of Cloud Connector administration UI</th>
<th>After fresh installation the Cloud Connector provides an initial user name and password and forces the user (Administrator) to change the password upon initial login.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Change the password of the Administrator user immediately after installation. Chose a strong password for the user (see [11]).</td>
</tr>
<tr>
<td></td>
<td>Configure a corporate LDAP system for the user management of the Cloud Connector administrator users. This guarantees that users of the Cloud Connector administration UI are named users and can be traced via the Cloud Connector audit log (see [13]).</td>
</tr>
<tr>
<td>Audit logging configuration in Cloud Connector</td>
<td>For end-to-end traceability of configuration changes in the Cloud Connector, as well as communication delivered by the Cloud Connector, it is recommended to switch on audit logging for productive scenarios.</td>
</tr>
<tr>
<td></td>
<td>Switch on audit log in Cloud Connector: set audit level to “All” (see [11], [7]).</td>
</tr>
<tr>
<td></td>
<td>Cloud Connector administrators are obliged to ensure that the audit log files are properly archived and do not get lost, in order to conform to the</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Running should be applied.</th>
<th>don’t reuse it for other scenarios.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use hard-drive encryption for the machine that runs the Cloud Connector. This ensures that the Cloud Connector configuration data cannot be read or modified by unauthorized users, even if they obtain access to the hard drive.</td>
</tr>
<tr>
<td></td>
<td>It is recommended that the audit log on operating system level is turned on to monitor the file operations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protection of Cloud Connector administration UI</th>
<th>After fresh installation the Cloud Connector provides an initial user name and password and forces the user (Administrator) to change the password upon initial login.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Change the password of the Administrator user immediately after installation. Chose a strong password for the user (see [11]).</td>
</tr>
<tr>
<td></td>
<td>Configure a corporate LDAP system for the user management of the Cloud Connector administrator users. This guarantees that users of the Cloud Connector administration UI are named users and can be traced via the Cloud Connector audit log (see [13]).</td>
</tr>
<tr>
<td>Audit logging configuration in Cloud Connector</td>
<td>For end-to-end traceability of configuration changes in the Cloud Connector, as well as communication delivered by the Cloud Connector, it is recommended to switch on audit logging for productive scenarios.</td>
</tr>
<tr>
<td></td>
<td>Switch on audit log in Cloud Connector: set audit level to “All” (see [11], [7]).</td>
</tr>
<tr>
<td></td>
<td>Cloud Connector administrators are obliged to ensure that the audit log files are properly archived and do not get lost, in order to conform to the</td>
</tr>
<tr>
<td><strong>SAP HANA Cloud Connector</strong></td>
<td><strong>Security Whitepaper</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Availability</td>
<td>To have end-to-end traceability, audit logging should also be switched on in the connected on-premise systems.</td>
</tr>
<tr>
<td><strong>Supported protocols</strong></td>
<td>Use the high availability feature of the Cloud Connector for productive scenarios (see [14]).</td>
</tr>
<tr>
<td></td>
<td>The route from the Cloud Connector to the on-premise system should be encrypted using SSL (for HTTPS) or SNC (for RFC).</td>
</tr>
<tr>
<td></td>
<td>Trust between the Cloud Connector and the connected on-premise systems should be established (see [15]).</td>
</tr>
<tr>
<td><strong>Configuration of on-premise systems in the Cloud Connector</strong></td>
<td>Use host name mapping of exposed on-premise systems (see [9]).</td>
</tr>
<tr>
<td></td>
<td>Narrow access to on-premise systems to resources required by the relevant cloud applications (see [9]).</td>
</tr>
<tr>
<td></td>
<td>Narrow list of cloud applications which are allowed to use the on-premise tunnel to the ones which need on-premise connectivity (see [15]).</td>
</tr>
<tr>
<td><strong>Usage of Cloud Connector instances for</strong></td>
<td>A single Cloud Connector instance can be used different Cloud Connector</td>
</tr>
</tbody>
</table>
productive and non-productive scenarios connected to multiple HCP accounts.
Accounts can be created by HCP users as a self-service. Different accounts are often used to separate dev, test and production.

It is recommended to not mix productive Cloud Connector usages with dev or test scenarios.

Instances to separate between productive and non-productive scenarios.

References

[1] SAP HANA Cloud Platform documentation

[2] HCP Connectivity Service documentation
https://help.hana.ondemand.com/help/frameset.htm?e54cc8fbbb571014beb5caaf6aa31280.html

[3] SAP HANA Cloud connector documentation
https://help.hana.ondemand.com/help/frameset.htm?e6c7616abb5710148cf3e75d96d596.html


[5] Information about SAP Data Centers
http://www.sapdatacenter.com/


[7] Audit logging in the Cloud connector

[8] Principal propagation through the Cloud connector
https://help.hana.ondemand.com/help/frameset.htm?d4d3e1e9b2dd44318b49a4812cd51383.html

[9] Access control configuration in the Cloud connector
https://help.hana.ondemand.com/help/frameset.htm?e7d4927dfbb571014af7ef6ebd6cc3511.html
https://help.hana.ondemand.com/help/frameset.htm?ca5868997e48468395cf0ca4882f5783.html

[10] Prerequisites to install the Cloud connector:
https://help.hana.ondemand.com/help/frameset.htm?e23f776e4d594fdaa1b1196d47b7e00.html

[11] Recommendations for secure setup of the Cloud connector:
https://help.hana.ondemand.com/help/frameset.htm?e7ea82a4bb5710144ce4eb61cb7e3d3f.html

[12] Replacing the SSL certificate of the Cloud connector administration UI by a trusted certificate:
https://help.hana.ondemand.com/help/frameset.htm?bdc5e5113c916ae8a443325692cd5b12.html

[13] Using LDAP for authentication of Cloud connector administration UI:
https://help.hana.ondemand.com/help/frameset.htm?120ceecfd84145a181ac160d588a7a3d.html

[14] Installing a failover instance for high availability:
https://help.hana.ondemand.com/help/frameset.htm?c697705179a24d2b8b6be038faff59c33.html

[15] Setting up trust between Cloud connector, on-premise systems and cloud applications:
https://help.hana.ondemand.com/help/frameset.htm?a4ee70f274248f8bbc7594179ef948d.html
Copyright

© Copyright 2014 SAP SE. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Oracle Corporation.

JavaScript is a registered trademark of Oracle Corporation, used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

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.