Security Challenges Associated With SAP HANA

Tom Schouten MSc RE CISSP CISA and Jan Stölting Dipl. Wirtschaftsinformatiker

Traditional risks associated with the technical security of SAP R/3 systems are generally unknown and neglected. SAP HANA introduces additional confidentiality, integrity and availability challenges to the SAP business suite. HANA is becoming the central data hub for interfaces and users, therefore logical access controls are vital for the security of the platform. The introduction of SAP HANA can be leveraged to eliminate previously neglected security vulnerabilities and offers the opportunity to design a holistic SAP security program.

Tom Schouten MSc RE CISSP CISA
is a manager at KPMG IT Advisory.
schouten.tom@kpmg.nl

Jan Stölting, Dipl. Wirtschaftsinformatiker,
is a manager at KPMG Cyber Security.
jstoelting@kpmg.com

Introduction

Due to the expanse of SAP functionalities and products, organizations are inadvertently increasing the number of access paths to their critical data assets. In addition, SAP embraces new technologies, which exposes SAP to all the security risks inherent to these technologies. Research has shown that these risks are only mitigated to a limited degree ([Scho13]).

This article studies the security implications associated with a recently introduced SAP technology, specifically related to in-memory performance technologies (HANA). An introduction to HANA will first be provided. After that, we study key changes to the IS/IT architecture and their impact on the SAP security concept. We conclude with a reflection on the recently released SAP security baselines and emphasize key security priorities.

SAP HANA

Companies reflecting on their future SAP landscape and strategy will engage with SAP S/4HANA (formerly: **H**igh Performance **An**alytic **A**ppliance). SAP Business Suite 4, or SAP HANA (hereafter: HANA), is the primary product of SAP's strategic growth initiative. The technological leap that accompanies HANA can be compared to the migration from R/2 to the currently known R/3 or the NetWeaver platform. As an in-memory, high performance data and application platform, HANA promises real-time business. Because data is stored in-memory (RAM), it can be directly accessed by analytic and transactional applications, that sit on top of HANA. From an architectural perspective, HANA can empower separate applications (e.g. SAP BW/BO) as a relational database in a classical 3-tier architecture or can be enabled to utilize the recently enabled SAP business suite S4/HANA. The eminent architectural novelties that HANA introduces (refer to Figure 1) require a revised view on the information security risks related to SAP. Before studying the impact on IS/IT security, we elaborate on major changes that the HANA technology introduces to the current SAP landscape in the section below.

Key Changes

HANA introduces major changes in terms of system architecture compared to SAP R/3 (that is supported by a classic database setup). We recognize two common change areas, based on the various HANA implementations studied:

1. Real-Time Analytical Access

The traditional separation between Online Analytical Processing (OLAP) systems, such as SAP BW, and Online Transaction Processing (OLTP) systems, such as SAP ECC is revoked. This improvement introduces real-time analytical access to transactional data, resulting in new use cases and (predictive) analytics scenarios or mobile applications. HANA is designed to be one (big) data layer/platform for all applications. Thus, HANA is connected to many more interfaces compared to the classic 3-tier architecture setup, in which the application server connects to the database using a communication user. In the case that HANA is used solely as a database, logical access controls are mainly focused on HANA's security-related features related to the restriction of (administrative) access.

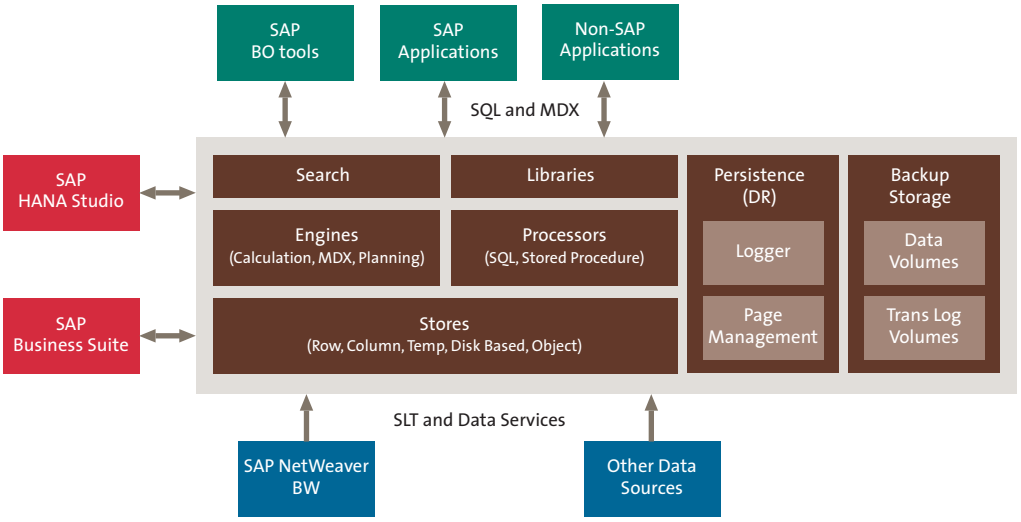

Figure 1. **SAP HANA architecture overview.**[1]

1 http://saptrainings.com/sap-hana-online-training/

2. Single Source of Truth – Data Layer

HANA is both an application and a data processing platform at the same time. Thus, the classical 3-tier architectural approach, i.e. separation of data presentation, processing and storage layers, become obsolete. Within HANA, the database is an integral part of the application. Therefore, new user groups, such as developers or end users, are very likely to work directly on the embedded database of HANA. Business logic, data processing and SAP program development is moved to the data layer. Consequently, all customized ABAP development needs to be rewritten to be highly performant. ABAP is the proprietary business programming language of SAP. The HANA platform can be considered as the future development platform for SAP programs.

The implementation of HANA introduces additional network channels, accounts, user groups, use cases and presents novel ways of accessing and developing SAP systems. HANA technology implicitly increase the attack surface to sensitive and critical data. As HANA is an application and data processing platform at the same time, the traditional 3-tier architecture and corresponding lines of defense are abandoned. Confidential data can be analyzed on a real-time basis, using well-known tools. The deployment of HANA inevitably requires a thorough risk analysis, assessment and treatment. An additional challenge is that the architectural changes are gradually evolving. HANA implementations usually start by enabling ERP on HANA, followed by the entire SAP (and non-SAP) systems running on HANA. Thus, the above-mentioned security risks are not necessarily applicable for a classical 3-tier architecture. However, it is vital to consider the future landscape when analyzing the risks and designing the security architecture during an initial HANA implementation. The next chapter provides guidelines, support and techniques on how to deal with these new security considerations.

Key Aspects

Most of the time software projects are driven by strong business needs and the provisioning of new, competitive functionality. The implementation of security requirements is often an afterthought within this process. A technology change, such as the implementation of HANA, provides companies with the perfect opportunity to implement previously dismissed security measures ([Scho13]).

Moreover, many companies lack a thorough understanding of the architectural and business process changes which HANA introduces. Often, HANA is perceived as "just another database" by the IT department thus overlooking the new use cases and associated risks. Our experience with HANA implementation projects show that the development of HANA information models and applications move closer to the business. This in turn requires awareness in secure development practices for a broader audience. Therefore, all employees should be aware of HANA becoming the central application and development platform, and the organizational changes and associated risks, in order to effectively implement and run SAP HANA.

To address security requirements and risks throughout the entire lifecycle of a HANA roll-out, the creation of a holistic SAP HANA security concept is required. SAP has released a HANA specific security guide which elaborates on HANA security configuration topics ([SAP15a]). Additionally in 2015, the SAP Security Baseline has been updated with the latest security recommendations for SAP HANA ([SAP15b]).

In Table 1, we have outlined a non-exhaustive list of recommended critical configuration settings that focus on common (neglected) security flaws that are required for a secure SAP HANA roll-out.

Area	Topic	Recommended control
Network and Communication Security	Network Security	Only dedicated and authorized network traffic should be allowed.
		Operate different components of the SAP HANA platform in different network zones.
		Restrict access to the SAP HANA interfaces.
	Secure Communication	Enable encryption for data in transfer for client-server and HANA internal communication.
General Hardening	Patch Management	The latest security patches should be applied for the SAP HANA system as well as the underlying operating system.
	Operating Systems (OS) users	Change the passwords of the standard OS users after hand-over of the SAP HANA appliance from the hardware vendor.
	Sensitive Information	Enable encryption of data at rest.
	Encryption Key Management	Initial default master keys, used within the Public Key Infrastructure (PKI) and SAP HANA, should be renewed ([ERPS15]).
Access Control	Identification	The user SYSTEM should be disabled for normal operational use and the initial password should be changed.
	Authentication	The password rules should be aligned to the Corporate Information Security Policy.
		Only SAP<SID> (technical account of application server) has a password with an unlimited lifetime.
	Authorization	Authorization concept should follow the "need-to-know" principle. See further in the next section.
Auditing	Audit Configuration	SAP HANA Auditing should be enabled for key activities.
	Securing the Audit Log	The audit log should not be tampered with by HANA admins. The privilege AUDIT OPERATOR should not be assigned to HANA admins.

Table 1. **Examples of recommended controls for a secure SAP HANA roll-out.**

While all of these topics are important, we would like to elaborate on the "Network and Communication Security" and "Access Control" areas in more detail as they are vital for the security of the platform and introduce significant changes to security.

Network Security

In order to implement a secure system, an overview of all the components that are connected to SAP HANA is necessary. Hence, a well-defined network topology or application architecture needs to be in place, which can be used to configure Access Control Lists (ACL). Network access to HANA should be restricted to dedicated, authorized communications channels only.

Access Control

Authentication

Well-known password parameters from the R/3 concept have been re-shaped within HANA security rules. A "password_layout" rule has been introduced to capture and verify password complexity requirements. The default value of this parameter "A1a" indicates that the password must contain one Uppercase, Numeric and Lowercase character as a minimum.

Authorization

Access controls are vital for the security of the platform due to the fact that far more users and systems have access to SAP HANA compared to traditional SAP databases. The fundament of controlling access to data in HANA is a detailed authorization concept.

In principle, access to a SAP HANA database is determined via the privileges granted to a user either directly or encapsulated within roles. Five different types of privileges can be distinguished:

1. SYSTEM privileges for administrative activities.
2. PACKAGE privileges for working with the SAP HANA repository.
3. OBJECT privileges for access to database objects such as the business schema holding the data.
4. Analytical privileges to further filter access to data provided by information models.
5. Application privileges for managing the access to an XS application (web application server running on the HANA platform).

In theory, high-level guidance for the development of an authorization concept is that HANA administrators mostly require SYSTEM privileges, information and role modelers require a combination of PACKAGE and OBJECT privileges (e.g. _SYS_BIC) and (business) users leveraging information models commonly require OBJECT and ANALYTICAL privileges.

Based on KPMG's good practices, several key principles can be applied for the definition of an appropriate authorization concept. This is a non-exhaustive list based on KPMG's proprietary knowledge:

1. Design should follow "need-to-know" principle.
2. Design Segregation of Duties (SoD) controls according to business needs.
3. Encapsulate privileges in roles which are designed in accordance to the job function.
4. Use repository roles instead of catalog roles. SAP HANA provides two different approaches for role modeling; repository roles and catalog roles. The usage of catalog roles should be avoided as these roles (1) are not transportable, (2) do not provide versioning, (3) require a super user for role management and provisioning and

(4) are owned by the user who creates them. This principle is not applicable to repository roles.
5. Develop (repository) roles in HANA development environment and use transport system for its transport into test and production systems.
6. Avoid the use of development rights in production (mostly granted via PACKAGE PRIVILEGES).
7. Avoid the use of pre-delivered SAP catalog roles such as MODELING.
8. Avoid the use of critical privileges such as ROLE ADMIN, _SYS_BI_CP_ALL and DEBUG.
9. Avoid the use of critical privilege combinations such as USER ADMIN and ROLE ADMIN.

Due to the introduction of HANA, Segregation of Duties matrices need to be updated to reflect the SAP HANA authorization design. Moreover, it is vital for the security of the whole system that technical interface/communication users follow the principle of least privilege, as HANA serves as the central data hub with numerous interfaces ([SAP14]).

Conclusion

A revised view on information security governance during the implementation of SAP HANA is required, due to the eminent architectural novelties that HANA introduces. The implementation of HANA results in the extension of sessions and implicitly introduces novel access paths to sensitive and critical information. As HANA is both an application and data processing platform, the traditional 3-tier architecture and corresponding lines of defense are abandoned. HANA becomes the central data hub for interfaces and users, therefore strong and/or granular access controls are vital for the security of the platform.

The fundament of controlling access to sensitive information in HANA is a detailed authorization concept and a revised authorization matrix. Additionally, an overview of all the components that communicate to SAP HANA is necessary. Hence, a well-defined application architecture needs to be in place, which can be used to restrict network access to dedicated, authorized communications channels only.

The implementation of HANA enables organizations to eliminate previously neglected security flaws and offers an opportunity to design a holistic SAP security concept. The HANA security guide and SAP security baseline should be included throughout the entire lifecycle of SAP HANA.

References

[ERPS15] ERPScan, Static encryption keys as the latest trend in SAP security, press release, June 18, 2015, http://erpscan.com/press-center/news/static-encryption-keys-as-the-latest-trend-in-sap-security/.

[SAP14] SAP, *How To... Define Standard Roles for Administrators and Developers in SAP HANA Database*, SAP How-to Guide, March, 2014, http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/c02c2004-899d-3110-8488-b3ff8362bbf6?QuickLink=index&overridelayout=true&59180354403522.

[SAP15a] SAP, *SAP HANA Security Guide*, July 1, 2015, http://help.sap.com/hana/sap_hana_security_guide_en.pdf.

[SAP15b] SAP, Security Baseline, May 5, 2015, https://service.sap.com/~sapdownload/012002523100003655872015E/Security_Baseline_Template.zip.

[Scho13] T. Schouten, *A False Sense of Security; Auditing (Beyond) the SAP Production System*, University of Amsterdam, 2013.

About the Authors

Tom Schouten MSc RE CISSP CISA is a manager at KPMG IT Advisory and is involved with, among other things, SAP security reviews, penetration testing, Continuous Auditing / Continuous Monitoring and compliance analytics. He is a multidisciplinary IT-audit professional supporting a wide range of (international) organizations.

Jan Stölting, Dipl. Wirtschaftsinformatiker, is a manager at KPMG Germany. He supports his clients in organizational as well as technical information security topics with a focus on application and database security, especially in the context of SAP. He has experience at various multinationals in the field of SAP HANA security & compliance and is author and lecturer in this area.

The fundament of controlling access to sensitive information in HANA is a detailed authorization concept and a revised authorization matrix