SAP HANA Security

Overview

SAP HANA SPS08

Andrea Kristen, Holger Mack, Tom Schröer (SAP SE)

July 2014

TABLE OF CONTENTS

1 DISCLAIMER

This document outlines our general product direction and should not be relied on in making a purchase decision. This document is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this document or to develop or release any functionality mentioned in this document. This document and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

2 SUMMARY

Protecting a company's or organization's critical data from unauthorized access and ensuring compliance with the growing number of rules and regulations is becoming increasingly important for SAP customers. SAP HANA® offers capabilities and benefits for customers in many important applications and scenarios and will therefore play an increasingly important part in many customers' critical IT and application infrastructures.

The purpose of this document is to give IT security experts a starting point and overview of what they need to understand about SAP HANA in order to comply with security-relevant regulations and policies and to protect their SAP HANA implementation and the data within from unauthorized access.

The document provides information on

- The impact of the different SAP HANA scenarios on how security needs to be addressed
- The framework and functions provided by SAP HANA that can be used to implement security and compliance requirements in line with the specific security, legal, and regulatory requirements
- How SAP HANA can be integrated into existing security infrastructures and processes
- Additional resources for more detailed information on SAP security topics

3 OVERVIEW AND SCENARIOS

3.1 Overview

SAP HANA is SAP's in-memory database technology that leverages hardware and software innovations to enable very fast processing of large amounts of data (for more details on SAP HANA see "Further reading"). SAP HANA can act as a standard SQL-based relational database. In this role it can serve as either the data provider for classical transactional applications (OLTP) and/or as the data source for analytical requests (OLAP). Database functionality is accessed through an SQL interface.

In addition, SAP HANA comes with a built-in application server, the "SAP HANA Extended Application Services (SAP HANA XS)". This server can be accessed through HTTP and can serve data via OData calls or rich HTML user interfaces.

In order to leverage the full potential of SAP HANA, data-intensive operations are executed directly in the database. Therefore SAP HANA provides a development/modeling environment that allows you to create new data structures and programs, analytical views and queries, stored procedures, and applications. The development environment is integrated into the SAP HANA studio, which also serves as the client tool for database administration or can be accessed via a browser interface. Design-time artifacts (like custom applications, roles, application content) are stored and managed in the SAP HANA built-in repository. Repository design time objects can be transported from development to quality assurance (QA) and production systems, using either SAP HANA's export/import functions or standard SAP mechanisms such as CTS+. Depending on the customer's requirements (for example size of the database), an SAP HANA system may consist of one host or a cluster of several hosts.

3.2 Deployment options

In on-premise deployments, SAP HANA is either delivered to customers as a standardized and highly optimized appliance, or customers can run SAP HANA in their own tailored server and storage combinations. Choosing the first option means that customers receive a completely installed and preconfigured SAP HANA system on certified hardware from an SAP hardware partner, including the underlying pre-installed and pre-configured operating system. The second option enables installed base customers to reduce hardware and operational costs, mitigate risk and optimize time-to-value, in addition to gaining additional flexibility in hardware vendor selection. For more information, see http://www.saphana.com/docs/DOC-3633.

There is a wide range of cloud offerings available for SAP HANA, from infrastructure- and platform-as-a-service to enterprise-class managed application hosting. For more information, see http://www.saphana.com/community/about-hana/deployment-options.

3.3 Availability

SAP HANA holds the bulk of its data in memory for maximum performance, but it still uses persistent storage to provide a fallback in case of failure. After a power failure, the database can be restarted like any disk-based database and returns to its last consistent state.

In addition, SAP HANA provides functionality for backup and recovery as well as high availability and disaster tolerance. These topics are described in separate documents (see "Further reading").

3.4 Scenarios

SAP HANA is used in different scenarios – for reporting and analytics in data marts, as a database in SAP NetWeaver Business Warehouse (SAP NetWeaver BW) and SAP Business Suite installations, and for providing database and application services to innovative new applications. This section will briefly introduce the different scenarios, how they differ from traditional security approaches and what customers need to consider from a security perspective when planning their SAP HANA projects. When planning the security of an SAP HANA implementation, it is important to understand the different scenarios and their impact. The scenarios below can also be combined within the same installation (with some restrictions).

3.4.1 Traditional 3-tier application

SAP HANA can be used as a relational database in a classical 3-tier architecture consisting of client – application server – database (see figure below). SAP HANA provides standard interfaces such as JDBC

and ODBC and supports standard SQL (with SAP HANA-specific extensions). For example, you can use SAP HANA as the database in an SAP NetWeaver Business Warehouse or SAP Business Suite installation.

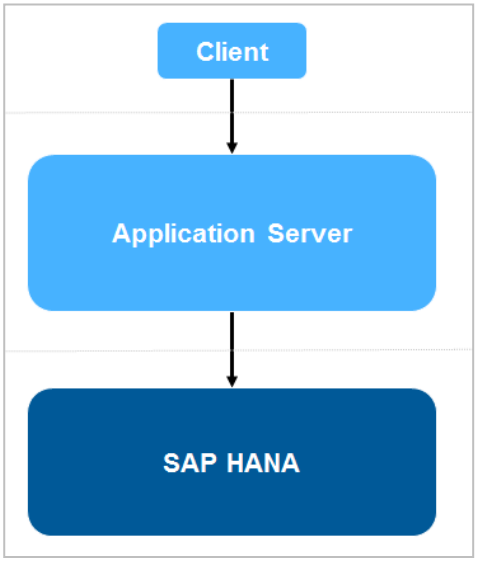

Figure 1: Traditional 3-tier application

Using SAP HANA in such an architecture does not change the existing security model or 3-tier architectures.

Security features such as authentication, authorization, user management, encryption, and audit logging continue to be located and enforced largely in the application server layer, while SAP HANA is used as the data store (with performance optimizations).

The application server connects to SAP HANA through a technical user account, and direct access to SAP HANA is only possible for database administrators. End users do not have direct access to either SAP HANA itself or the server on which it is running. As a consequence, SAP HANA security functions are used mainly to manage administrative access..

SAP Business Suite on HANA or SAP Business Warehouse on HANA are examples for such architectures.

3.4.2 Data mart for analytics (3-tier or 2-tier)

SAP HANA was first used in scenarios that focus on analytical use cases. In these scenarios, data is typically replicated from a source system such as SAP Business Suite into SAP HANA. Customer-specific reports and dashboards provide direct read-only access to data in SAP HANA (2-tier architecture), with the option to use a wide range of BI tools incl. SAP BusinessObjects Intelligence (usually 3-tier architecture), see figure below.

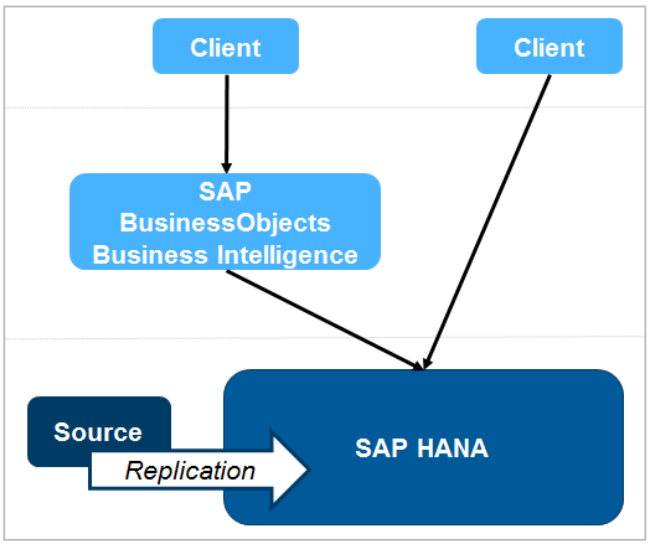

Figure 2: Data mart for analytics (3-tier or 2-tier)

This architecture requires a project-specific security model.

End users need to exist in SAP HANA's identity store. Authorization checks are carried out using SAP HANA privileges (modelled for the individual project), which need to be granted to the end users in SAP HANA. The security features provided by SAP HANA are described in the section "Security functions".

3.4.3 Native 2-tier application

SAP HANA Extended Application Services (SAP HANA XS) embed a full-featured application server, web server, and development environment within SAP HANA itself. Applications can be deployed directly on SAP HANA XS, which exposes the applications to end users via a web interface (2-tier architecture), see figure below.

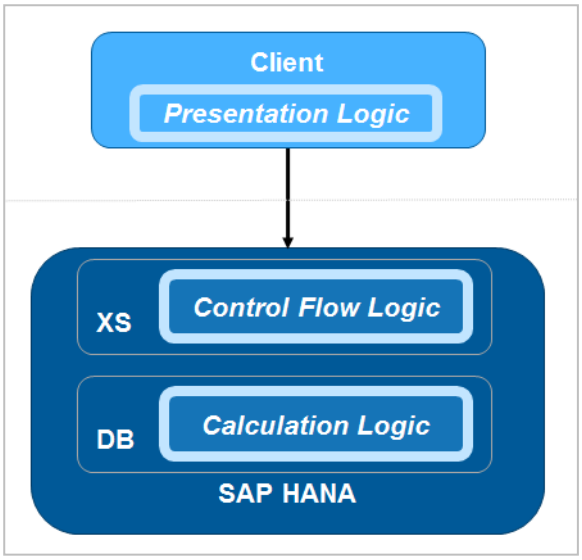

Figure 3: Native 2-tier application

As SAP HANA XS is part of SAP HANA, it also shares the same security model.

This means that the majority of security features described in the section "Security functions" apply directly to XS-based applications, with some minor differences for example in the supported authentication methods. Additionally, SAP HANA XS contains support for protection against typical vulnerabilities of web-based applications, for example XSRF. Details and recommendations for developing secure applications on SAP HANA can be found in the SAP HANA Developer Guide (see "Further reading").

4 SECURITY FUNCTIONS

SAP HANA provides security functions that enable customers to implement different security policies and meet compliance requirements. This section provides an overview of SAP HANA's security functions. Depending on the scenario in which SAP HANA is used (see "Overview and scenarios"), only some of these functions might actually be needed; others might be used in other architecture layers.

For detailed information please refer to the SAP HANA Security Guide (http://help.sap.com/hana/SAP_HANA_Security_Guide_en.pdf).

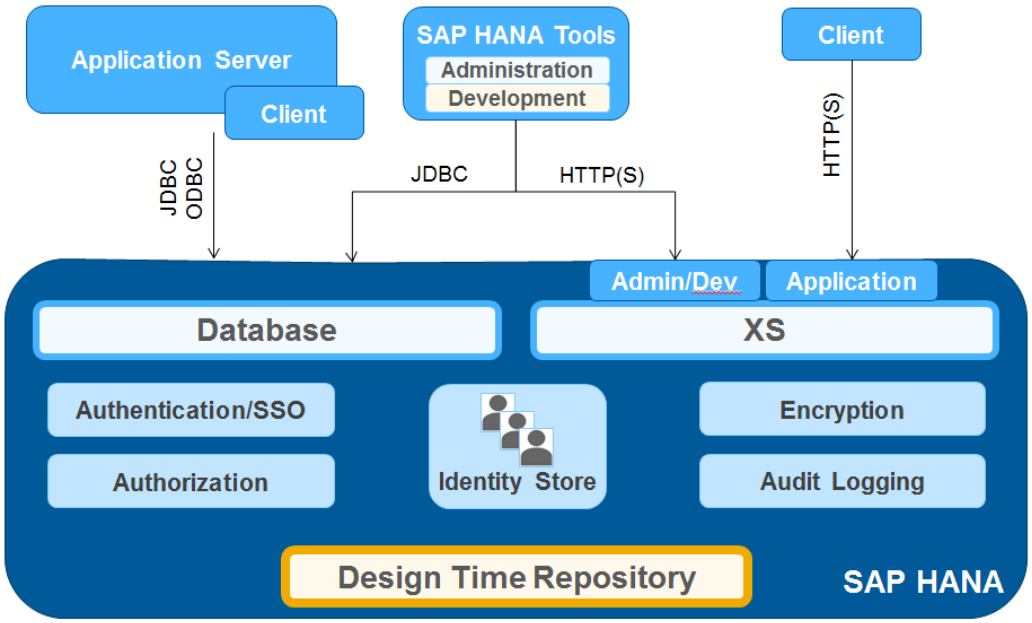

Figure 4: SAP HANA security function overview

4.1 Authentication and single sign-on

Access to SAP HANA data and applications requires authentication. Several authentication methods are available.

Authentication method	Available for access via JDBC/ODBC	Available for access via HTTP (SAP HANA XS)
User name/password Password policies, for example password length and complexity, can be defined	Yes	Yes (basic authentication, form-based login)
Kerberos	Yes	Yes (SPNEGO)
SAML 2.0	Yes (bearer token)	Yes
SAP logon/assertion tickets	Yes	Yes
X.509	-	Yes

Table 1: SAP HANA authentication methods

4.2 User and role management

To be able to log on to SAP HANA, a user must exist in the identity store of SAP HANA. Depending on the scenario, the user accessing SAP HANA can either be a technical account, a database administrator, or an individual end user.

The actions that a user can perform depend on the roles and privileges that were assigned to the user. Roles are used to bundle and structure privileges, allowing you to create sets of privileges for dedicated user groups.

Role designers can create roles in the SAP HANA repository of a development system, from where they can then be transported to the production system. This makes it possible to separate role design from transport and from later role assignment to end users, see figure below.

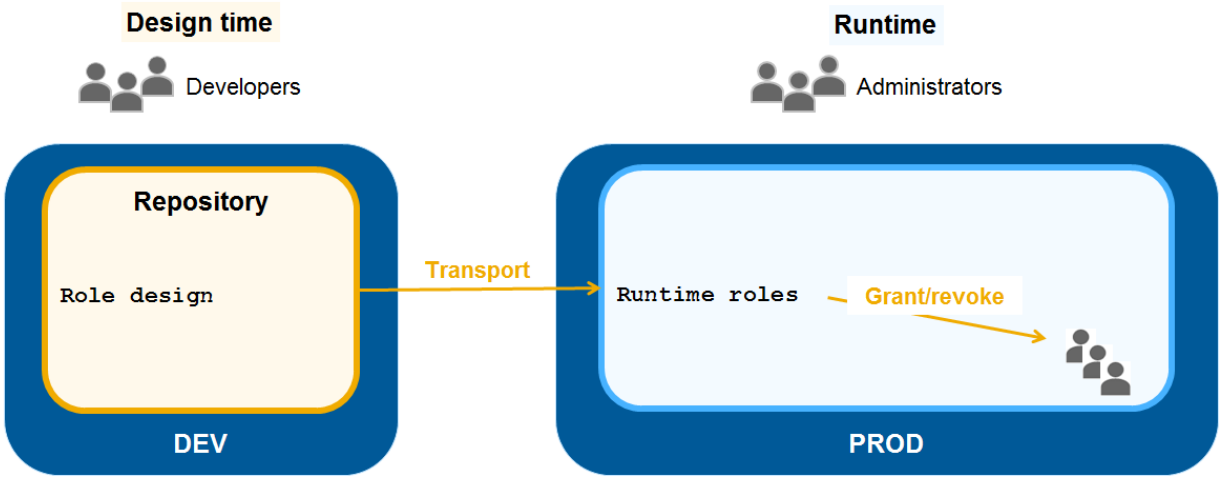

Figure 5: Role lifecycle

For user administration and role assignment, administrators can use either the SAP HANA studio (GUI) or SQL commands. Adapters for SAP NetWeaver Identity Management and GRC Access Control are available to allow integration into existing user provisioning infrastructures.

4.3 Authorization framework

SAP HANA provides a rich set of authorization mechanisms based on standard SQL privileges and SAP HANA-specific extensions for business applications.

All access to data and execution of actions in SAP HANA require authorization: privileges control what users can do. Privileges can be assigned to both roles and users. It is recommended to bundle privileges into roles. Best practice information and role templates are available in the following document: https://scn.sap.com/docs/DOC-53974

Privilege type	Target users	Description
System privileges	Administrators	For database access Authorize execution of administrative actions for the whole SAP HANA system
SQL privileges	Technical user accounts, end users (depends on architecture)	For database access Authorize access to data and operations on individual database objects

Privilege type	Target users	Description
Analytic privileges	Technical user accounts, end users (depends on architecture)	For database access Authorize read access on analytic views at run-time, provide row-level access control based on the attributes of the relevant view
Application privileges	End users	For application access Authorize access to SAP HANA XS application functions
Repository privileges	Developers	For repository access Authorize access in the repository (modeling environment) at design time

Table 2: SAP HANA privilege types

4.4 Communication and data encryption

SAP HANA supports SSL connection encryption: for connections between SAP HANA and clients, between the nodes within an SAP HANA scale-out system, and also between SAP HANA systems in different data centers (failover scenarios).

Although SAP HANA holds the bulk of its data in memory for maximum performance, it still uses persistent storage ("data volumes") to provide a fallback in case of failure. After a power failure, the database can be restarted like any disk-based database and returns to its last consistent state. SAP HANA can encrypt the data volumes on disk.

For backup encryption, a wide range of 3rd party backup tools has been certified for use with SAP HANA (see Further reading).

4.5 Audit logging

Audit logging allows to track actions performed in SAP HANA: who did what – or tried to do what – and when. Customer-specific audit policies can be created in SAP HANA Studio or using SQL statements.

SAP HANA provides audit logging for critical security events, such as changes to roles and user privileges or the system configuration. It can also log access to sensitive data: write and read access to objects such as tables or views, as well as the execution of procedures. Firefighter logging is available, which makes it possible to track all actions of a specified user (for example if a support user needs high-privilege access to a production system).

You can choose whether the audit trail is written to Linux syslog or to a database table within SAP HANA itself:

- Linux syslog enables easy integration into existing monitoring and auditing infrastructures, and can be configured to write the audit trail to remote servers, thus enabling a physical segregation of database administration and audit log analysis.
- Using an SAP HANA database table as the target for the audit trail makes it possible to query and analyze auditing information quickly. It also provides a secure and tamper-proof storage location.

4.6 Security administration

SAP HANA Studio is the main administration and development tool for SAP HANA. It is Eclipse-based and provides different perspectives for different use cases:

- Administration Console: Runtime security configuration, user/role and authorization management, monitoring, audit logging configuration
- Development/Modeler: Design time security definition, role and analytic privilege design, application-specific security definition

Alternatively, most security administration tasks can be carried out using SQL commands. SAP HANA has also been integrated into DBA Cockpit (part of SAP NetWeaver).

Additionally, the following web-based tools are available for SAP HANA:

- XS Administration Tool: Web-based administration tool for XS-specific security configuration, application-specific runtime security configuration
- Web IDE: Web-based development environment for XS applications

5 INFRASTRUCTURE INTEGRATION

SAP HANA supports standard and documented interfaces to enable integration with customer security network and datacenter infrastructures.

- Identity management (user and role provisioning)
  - SQL-based interface for user and role creation
  - Adapter for SAP NetWeaver Identity Management
- Compliance infrastructure
  - Adapter for SAP Access Control
- Standards-based single sign-on infrastructures based on Kerberos (for example Microsoft Active Directory) and SAML
- Logging/monitoring infrastructures
  - Database audit trail can be written to Linux syslog

Further details can be found in the SAP HANA Security Guide (see “Further reading”)

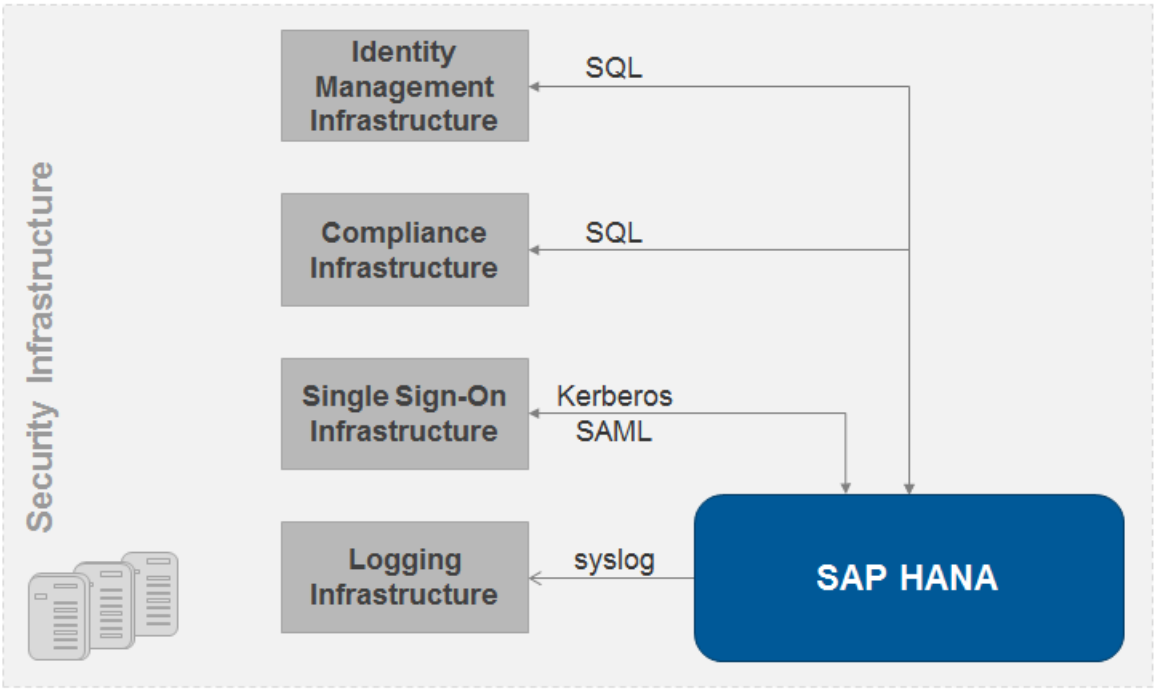

Figure 6: SAP HANA data center integration

5.1 Security patches

SAP HANA security patch information is published as part of the general SAP security patch strategy (SAP Security Notes). SAP HANA security patches are delivered as SAP HANA revisions and can be applied using the SAP HANA Software Lifecycle Manager (HDBLCM).

5.2 Network

The network communication channels (purpose, ports) used by SAP HANA are documented in detail in the SAP HANA Master Guide. The SAP HANA Security Guide includes recommendations on the use of firewalls, for example to separate internal and external communication as well as the options for encryption using SSL. A reference of the SAP HANA SQL command network protocol is also available. Fore more information, see “Further reading”

5.3 Supporting compliance requirements

Compliance plays an important role in many customer environments. Compliance in most cases is not a product feature, but depends on many factors such as relevant rules and regulations (IT policies, industry, country, and so on), already existing technology/infrastructure, and customers' processes and audit approach.

SAP HANA provides functions that support customers in achieving compliance:

- Best practices in security operations
- Need-to-know principle, separation of duties on all levels
- Control of privileged access
- Ability to audit
- Deletion of data

SAP HANA takes an end-to-end approach, the basis for which is provided by the built-in security functions and secure pre-configuration of the SAP HANA software and hardware stack.

This is extended by SAP HANA's integration into existing security infrastructures through standard/documented interfaces and the option to use 3rd-party tools for data center operations.

Last but not least SAP HANA provides end-to-end documentation for the whole software lifecycle, including an extended security guide and recommendations on secure setup and operation.

6 FURTHER READING

- SAP HANA documentation on SAP Help Portal at http://help.sap.com/hana_platform
  - SAP HANA Security Guide
  - SAP HANA Administration Guide (step-by-step instruction, also covers backup/recovery and high-availability/disaster tolerance)
  - SAP HANA Master Guide (contains information on network topics)
  - SAP HANA Developer Guide (contains secure programming guidelines for SAP HANA-based applications)
  - SAP HANA SQL and System Views Reference
  - SAP HANA SQL Command Network Protocol
- Best practice document on SAP HANA roles (incl. role templates): https://scn.sap.com/docs/DOC-53974
- SAP HANA tailored data center options: http://www.saphana.com/docs/DOC-3633
- SAP HANA deployment options: http://www.saphana.com/community/about-hana/deployment-options
- Information on 3rd party backup tools certified for SAP HANA: http://www.saphana.com/community/blogs/blog/2012/12/19/backint-for-sap-hana-certification-available-now
- Central SAP HANA website: http://www.saphana.com
- SAP HANA Academy: http://www.saphana.com/community/implement/hana-academy
- Hasso Plattner, In-Memory Data Management: An Inflection Point for Enterprise Applications (2011)