SAP HANA Security

Whitepaper

SAP HANA SPS11

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

February 2016

TABLE OF CONTENTS

Contents

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.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company 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.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

1 SUMMARY

Protecting a company’s or an 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 plays 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 concepts in line with the specific security, legal, and regulatory requirements
- How SAP HANA can be integrated into existing security infrastructures and processes
- SAP’s secure software development process and the security patch strategy

2 INTRODUCTION

2.1 What is SAP HANA?

SAP HANA is an in-memory platform that combines an ACID-compliant database with advanced data processing, application services, and flexible data integration services. 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 can also be used as an application platform. Two options are available for this: SAP HANA extended application services, classic model is an application server directly built into SAP HANA, which can be accessed through HTTP and serve data via OData calls or rich HTML user interfaces. SAP HANA extended application services, advanced model is a new option that provides a separate application platform layer and supports a broader variety of programming languages. Extended application services in general are referred to as XS.

SAP HANA supports multiple isolated databases within a single SAP HANA system via multitenant database containers (MDC). All the databases in a multiple-container system share the same installation of the database system software, the same computing resources, and the same system administration. However, each database in such a system is self-contained and isolated, for example with regard to its users, data, backups, and trace files.

A SAP HANA system may consist of one host or a cluster of several hosts (“scale-out system”).

For more information on SAP HANA in general, see “Further reading”.

2.2 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 hardware setup. 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 and optimize time-to-value, in addition to gaining additional flexibility in hardware vendor selection.

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 “Further reading”.

2.3 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 SCENARIOS

SAP HANA is used in different scenarios – as a database in SAP Business Warehouse (SAP BW), SAP Business Suite and S4HANA installations, for reporting and analytics in data marts, and as an application platform. 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. The scenarios below can also be combined within the same installation (with some restrictions).

3.1 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 for SAP Business Warehouse, SAP Business Suite or S4HANA.

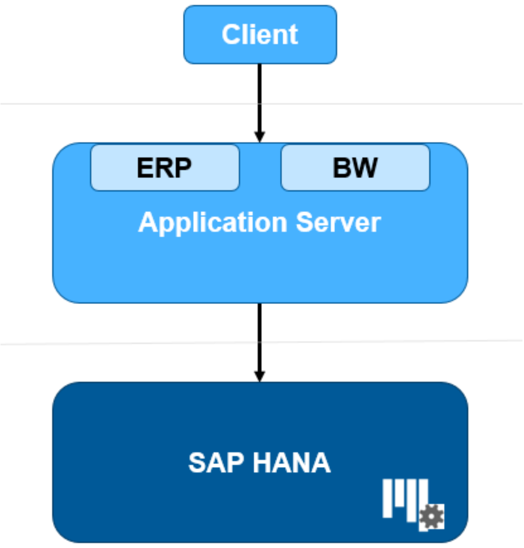

Figure 1: 3-tier application

Using SAP HANA as a database in such scenarios does not change the traditional security model of 3-tier architectures.

Security features such as authentication, authorization, user management, encryption, and audit logging are mainly provided and enforced in the application server layer, while SAP HANA is used as a data store only (with performance optimizations).

The application server connects to SAP HANA through a technical user account. 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.

3.2 Application on SAP HANA extended application services, classic model

SAP HANA extended application services, classic model embed a full-featured application server, web server, and development environment within SAP HANA itself. Applications can be deployed directly on SAP HANA extended application services, classic model. They are exposed to end users via a web interface (2-tier architecture), see figure below.

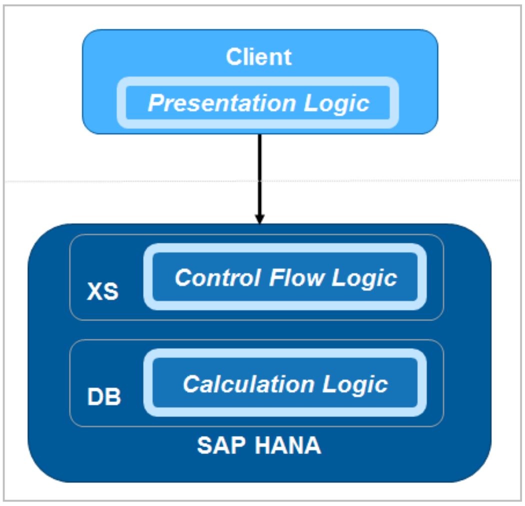

Figure 2: Application on SAP HANA extended application services, classic model

As SAP HANA extended application services, classic model are part of SAP HANA, the same security model applies.

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

3.3 Application on SAP HANA extended application services, advanced model

As of SAP HANA SPS11, SAP HANA extended application services, advanced model are available as an additional option. The overall architecture is less intertwined with SAP HANA in general, which brings more deployment options.

One option is to install SAP HANA extended application services, advanced model directly on the SAP HANA server, but an installation on a separate host from the SAP HANA database is also possible. This can be done to scale XS independent of the database, as you can have many more XS nodes than SAP HANA database nodes.

This change in architecture has impact on some security aspects of applications or operations of SAP HANA, for example you can install SAP HANA extended application services, advanced model in a separate network from SAP HANA itself, which makes it possible to put XS into a DMZ and have a firewall between the XS and database layers. Additionally new concepts for user and authorization management are supported (see “Further reading”).

3.4 Integrated scenario: reporting on ERP data in SAP HANA

SAP HANA Live for SAP Business Suite supports direct access to ERP data in SAP HANA. ERP data is exposed via virtual data models (SAP HANA views), which are read-only and can be adapted by customers. Authorization checks for direct access are done using SAP HANA privileges. There is tool support for generating SAP HANA privileges from ABAP PFCG roles (SAP HANA Studio plugin) and for generating SAP HANA users directly from existing ABAP users (SU01).

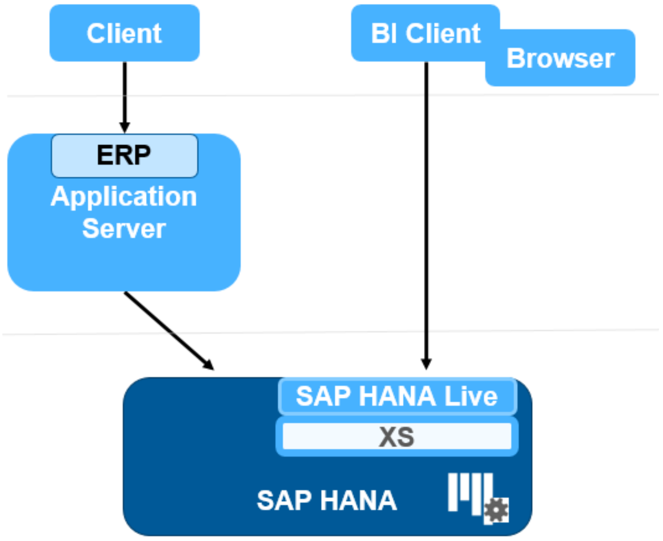

Figure 3: Reporting on ERP data in SAP HANA

3.5 Integrated scenario: reporting on BW data in SAP HANA

SAP Business Warehouse supports direct access to BW data in SAP HANA. BW data is exposed via special info providers (SAP HANA views), which are read-only. Authorization checks for direct access are done using SAP HANA privileges. BW provides automatic generation of SAP HANA views, privileges and roles based on BW privileges. SAP HANA users can be generated directly from existing ABAP users (SU01), and BW can automatically assign the correct SAP HANA roles to them.

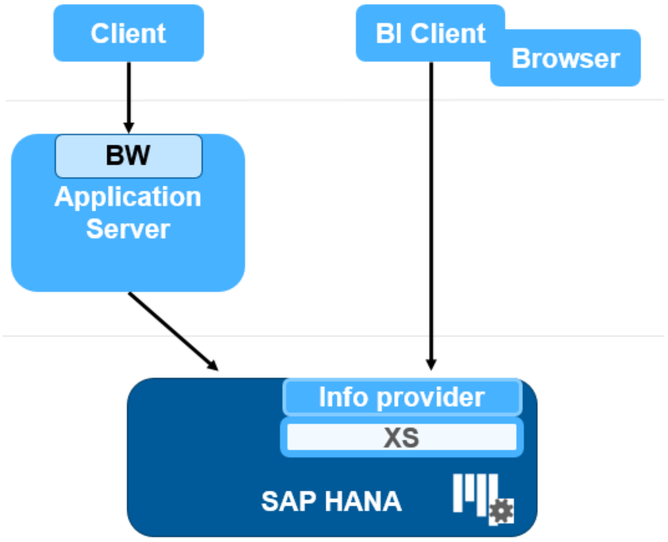

Figure 4: Reporting on BW data in SAP HANA

3.6 Data mart: customer-specific analytic reporting on SAP HANA

Other typical SAP HANA use cases focus on analytic reporting. In these scenarios, data is usually replicated from a source system such as SAP Business Suite into SAP HANA. Customer-specific reports and dashboards provide direct read-only access to this data in SAP HANA, with the option to use a wide range of BI tools including SAP BusinessObjects Intelligence.

This architecture requires a project-specific security model. 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 functions provided by SAP HANA are described in the section “Security functions”.

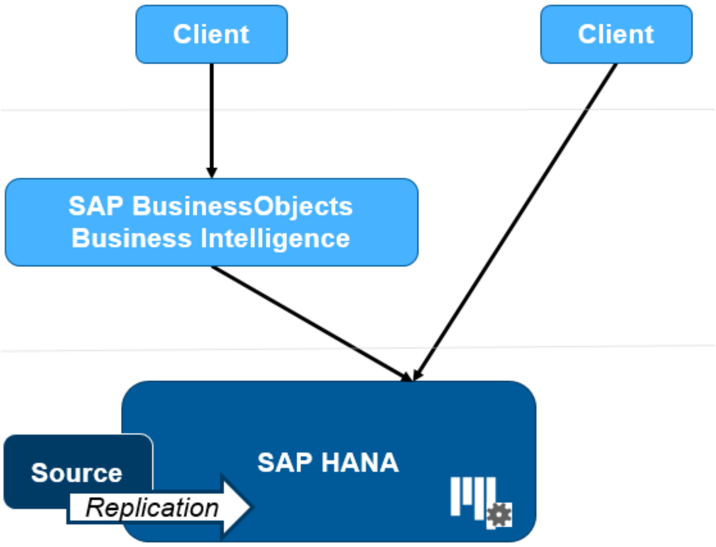

Figure 5: Data mart

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 "Scenarios"), only some of these SAP HANA security functions might actually be needed, while others might be provided by different architecture layers.

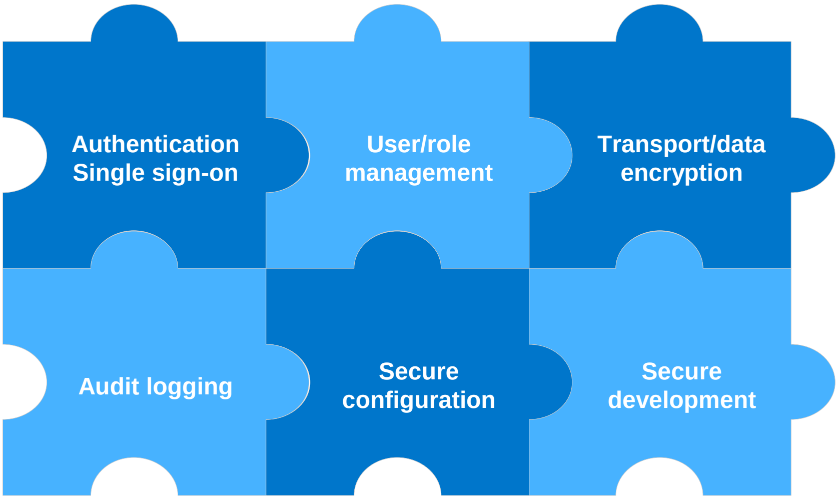

Figure 6: SAP HANA security function overview

Detailed information on the available security functions can be found in the SAP HANA Security Guide, see "Further reading".

4.1 Access control

4.1.1 User management

Depending on the scenario, the user accessing SAP HANA can either be a technical account, a database administrator, or an individual end user.

For user administration and role assignment, administrators can use SAP HANA tools. There are also adapters for SAP Identity Management and GRC Access Control, which allow integration into existing user provisioning infrastructures. To connect custom user provisioning solutions, SAP HANA's SQL interface can be used. User self services e.g. for web-based password reset or new user account requests are also available.

4.1.2 Authentication and single sign-on

Access to SAP HANA data, functions and applications requires authentication. SAP HANA offers several authentication options, which can be configured per user.

For password login, a password policy governs change frequency, password complexity and other password-related security settings. SAP HANA does not use default passwords. After first logon, users are forced to set new passwords.

Several single sign-on options are available: Kerberos/SPNEGO, SAML, SAP logon and assertion tickets, X.509 (only SAP HANA extended application services, classic model).

4.1.3 Authorization framework

The actions that a user can perform depend on the assigned roles and privileges. Roles are used to bundle and structure privileges, allowing to create sets of privileges for dedicated user groups. Best practice information and role templates are available (see "Further reading").

Role designers can create roles in the SAP HANA built-in 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 role assignment to end users, see figure below.

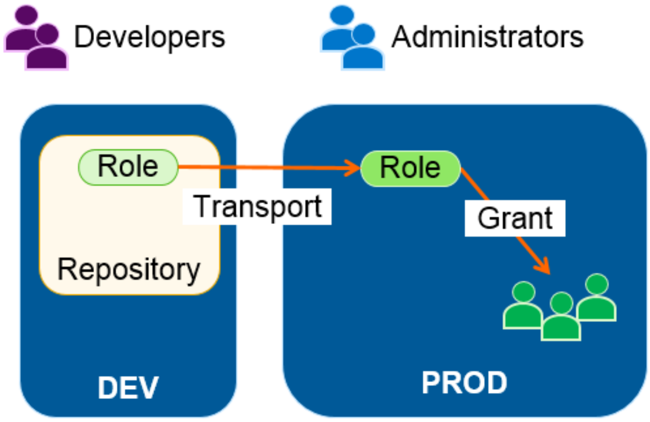

Figure 7: Role lifecycle

SAP HANA privileges are based on standard SQL privileges and SAP HANA-specific extensions for business applications. The following table gives an overview of the different privilege types.

Target users	Description
End users	Access to database content, e.g. SELECT on table → SQL privileges, analytic privileges Execution of native application functions → XS application privileges (SAP HANA extended application services, classic model)
Administrators	Execution of administration tasks e.g. backups or user management → system privileges
Developers	Access to development artifacts in the repository → package privileges

Table 1: SAP HANA privilege types

Applications running on SAP HANA extended application services, advanced model use a new authorization concept. For more information see “Further reading”.

4.1.4 Audit logging

Audit logging records critical system events, for example changes to roles and users or the database configuration. It can also record access to sensitive data: write and read access to objects such as tables or views, as well as the execution of procedures. For situations where a highly privileged user needs temporary access to a critical system, “firefighter” logging can be enabled, which tracks all actions of a specific user.

Both successful and unsuccessful actions can be recorded.

The recorded events can either be written to Linux syslog or to a secure database table within SAP HANA:

- 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 the secure 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.

4.2 Secure configuration and encryption

SAP HANA comes with secure defaults. Note that configuration settings allow you to customize your system for your implementation scenario and system environment. Some of these settings are specifically important for the security of your system, and misconfiguration could leave your system vulnerable.

A security checklist of critical configuration settings is provided in the SAP HANA Security Guide. For monitoring security-related settings, administrators can use both SAP HANA tools (alerts in SAP HANA Studio, security dashboard in SAP HANA Cockpit) and standard SAP tools such as SAP Early Watch Alert or System Recommendation.

It is strongly recommended to verify systems for critical configurations and to always apply the latest security patches.

4.2.1 Communication channel encryption

SAP HANA supports TLS connection encryption for network communication channels.

Encryption of client-server communication (external channels) can be enforced.

For internal channels a public-key infrastructure (PKI) is automatically set up during installation. Internal channels include connections between the nodes of an SAP HANA scale-out system, between SAP HANA systems in system replication scenarios, and between hot and warm store in dynamic tiering scenarios.

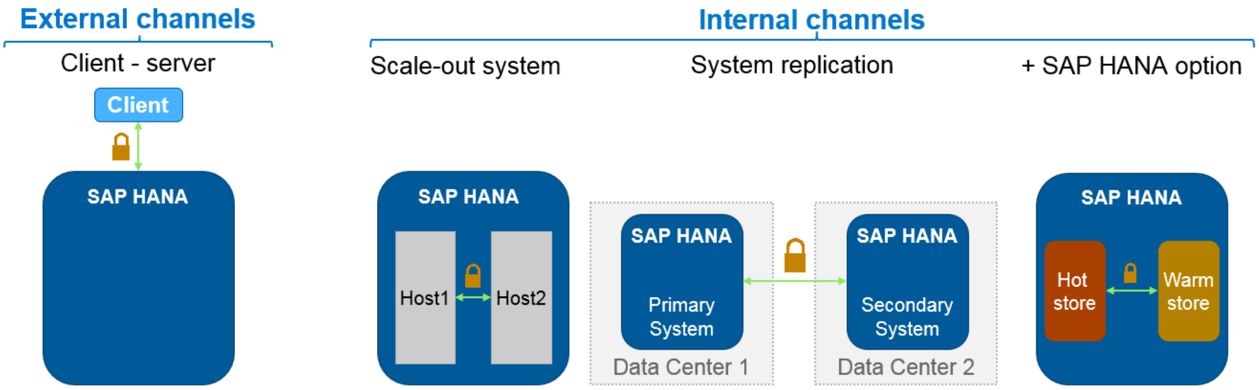

Figure 8: SAP HANA communication channels

The network communication channels (purpose, ports) used by SAP HANA are documented in detail. This includes recommendations on the use of firewalls and network zones, for example how to separate internal and external communication. A reference of the SAP HANA SQL command network protocol is also available. For more information, see “Further reading”.

4.2.2 Data encryption

While authorization is the primary means for fine-granular access control, encryption addresses a potential bypass of authorization on lower architecture layers.

Different encryption options are available when using a SAP HANA system:

- Data at rest encryption: although SAP HANA holds the bulk of its data in memory for maximum performance, it still uses persistent storage (data files) to provide a fallback in case of failure. These data files can be encrypted.
- Application encryption: encryption APIs are available for XS applications
- Backup encryption: a wide variety of 3rd party backup tools are certified for SAP HANA’s Backint interface, which provide advanced backup encryption and key management capabilities, see “Further reading”.

SAP HANA uses SAP’s standard cryptographic library, which is FIPS-certified.

4.3 Tools and data center integration

4.3.1 SAP tools

SAP HANA Studio is the main administration and monitoring tool for SAP HANA. The Administration perspective is used to maintain the runtime security configuration, manage users, roles and authorization, monitor security and configure audit logging. In the Development/Modeler perspective, design time security definitions such as roles and analytic privileges are created and tested, and security functions for applications on SAP HANA extended application services, classic model can be developed.

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

- SAP HANA Cockpit: New administration and monitoring tool for SAP HANA, which contains a dedicated security dashboard for monitoring security KPIs and maintaining the security configuration
- SAP HANA Web-Based Development Workbench: development environment for applications on SAP HANA extended application services, classic model and web-based user and role management for all XS applications

SAP HANA has also been integrated with SAP Solution Manager: DBA Cockpit for database management, Early Watch Alert, System Optimization Services and System Recommendation.

User and role provisioning can also be carried out via SAP Identity Management (adapter available). SAP Access Control also supports SAP HANA.

For database activity monitoring, SAP Enterprise Threat Detection is available.

4.3.2 Interfaces and 3rd party tool support

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

Most security administration tasks can be carried out using SQL commands, for example identity management (user and role provisioning) or compliance-related activities (checking critical authorization combinations). Standards-based single sign-on is available via Kerberos (for example Microsoft Active Directory) and SAML. For integration into an enterprise logging infrastructure, SAP HANA audit logging supports Linux syslog. Antivirus software can be used for XS applications via a dedicated antivirus interface.

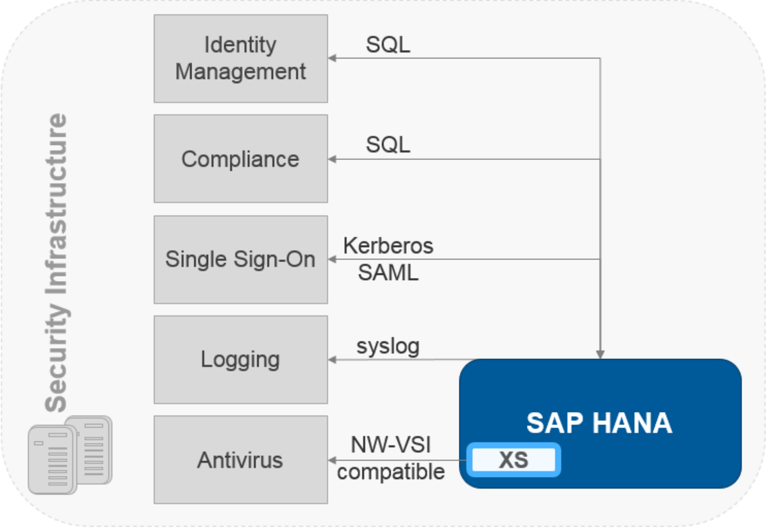

Figure 9: SAP HANA data center integration

In general, installing 3rd party tools on SAP HANA is supported if they comply with the following SAP Notes:

- 1730928: Using external software in a HANA appliance
- 1730929: Using external tools in an SAP HANA appliance
- 1730930: Using antivirus software in an SAP HANA appliance
- 1730932: Using backup tools with Backint
- 1730999: Configuration changes in HANA appliance
- 784391:   SAP support terms and 3rd-party Linux kernel drivers

5 SECURITY IN THE SOFTWARE LIFECYCLE

5.1 Secure development

SAP has a comprehensive product security strategy across the enterprise that rests on three pillars: Prevent – React – Detect. An important component of this strategy is the Secure Development Lifecycle, which provides a comprehensive framework of processes, guidelines, tools and staff training, and ensures that security is an integral component for architecture, design and implementation of SAP solutions.

The Secure Development Lifecycle is a threat-based approach, which includes comprehensive security testing including automated and manual tests.

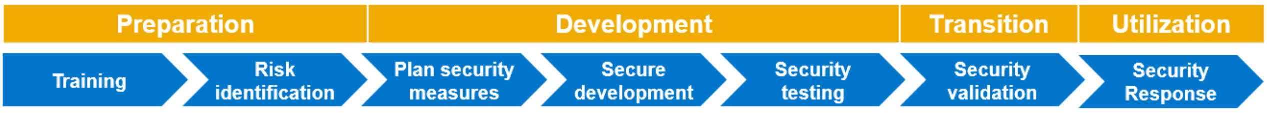

Figure 10: Secure software development lifecycle

5.2 Security patches

Information about SAP HANA security patches is published according to the general SAP security patch strategy in SAP security notes, see “Further reading”.

http://service.sap.com/securitynotes → for SAP HANA, filter for component HAN*

Security patches are delivered as SAP HANA revisions and can be applied using SAP HANA’s lifecycle management tools. Operating system patches are provided by the respective operating system vendors.

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 instructions, also covers backup/recovery and high-availability/disaster tolerance)
    - SAP HANA Master Guide (includes information on network topics)
    - SAP HANA Developer Information Map (includes secure application programming guidelines)
    - SAP HANA Developer Guide for SAP HANA XS Advanced Model
    - SAP HANA SQL and System Views Reference
    - SAP HANA SQL Command Network Protocol
- Secure configuration
    - SAP HANA security configuration checklist (part of the Security Guide)
    - SAP Security Baseline Template
    - DSAG Prüfleitfaden ERP 6.0
- Best practice document on SAP HANA roles (incl. role templates): https://scn.sap.com/docs/DOC-53974
- SAP HANA tailored data center: https://blogs.saphana.com/2015/02/18/sap-hana-tailored-data-center-integration-tdi-overview/
- SAP HANA deployment options: http://hana.sap.com/platform.html
- Information on 3rd party backup tools certified for SAP HANA: https://scn.sap.com/docs/DOC-62799
- FIPS certification of SAP's cryptographic library: http://scn.sap.com/community/security/blog/2015/01/21/sap-s-crypto-kernel-receives-fips-140-2-certificate
- Security notes and patches:
    - FAQ SAP Security Notes
    - SAP HANA revision strategy
- SAP security approach:
    - http://www.sap.com/security
- SAP HANA information on SCN: http://scn.sap.com/community/hana-in-memory
- Central SAP HANA website: http://hana.sap.com
- SAP HANA Academy: https://www.youtube.com/user/saphanaacademy
- Hasso Plattner, In-Memory Data Management: Technology and Applications (2012)