



PUBLIC

# **SAP HANA Security**

## Technical Whitepaper

March 2021

**THE BEST RUN**



# TABLE OF CONTENTS

|   |    |
|---|----|
| WHAT IS SAP HANA?   | 4  |
| Availability  | 4  |
| Deployment options  | 5  |
| On-premise deployments                                      | 5  |
| Cloud deployments   | 5  |
| SCENARIOS DETERMINE THE SECURITY APPROACH                   | 6  |
| SAP HANA as a database in 3-tier scenarios                  | 6  |
| Data marts: customer-specific analytic reporting            | 7  |
| Integrated scenarios  | 8  |
| Application development                                     | 8  |
| SECURE DATA AND APPLICATIONS                                | 9  |
| User and identity management                                | 10 |
| Authentication and single sign-on                           | 10 |
| Authorization and role management                           | 11 |
| Shared SAP business application authorizations              | 12 |
| Masking   | 13 |
| Data anonymization  | 13 |
| Encryption  | 14 |
| Backup encryption   | 14 |
| Data and log encryption                                     | 14 |
| Column encryption   | 15 |
| Application encryption                                      | 15 |
| Encryption configuration and key management                 | 15 |
| Communication encryption: TLS/SSL                           | 16 |
| Auditing  | 16 |
| SECURE SETUP  | 17 |
| Default multi-tenancy mode                                  | 17 |
| Security information  | 18 |
| Tools for security configuration, management and monitoring | 18 |
| Interfaces and 3rd party tool support                       | 19 |
| Data protection and privacy                                 | 20 |
| SECURE SOFTWARE   | 21 |
| Secure development  | 21 |
| Security patches  | 21 |
| FURTHER READING   | 22 |

Innovate with confidence on SAP HANA. Data is at the core of today's digitized economy, constantly increasing not only in volume, but also in value and importance to businesses. Protecting a company's critical data from unauthorized access and ensuring compliance with the growing number of security, legal and regulatory requirements (e.g. GDPR) is therefore a top concern for business leaders. With SAP HANA's built-in security, you can take advantage of the latest innovations while staying in control of the security and compliance of your data throughout your digital transformation journey.

SAP HANA is designed as a multi-purpose business data platform for the intelligent enterprise, which supports analytical and transactional scenarios in different deployment modes on premise and in the cloud. SAP HANA's comprehensive security approach enables customers to address all security aspects of such a multipurpose platform:

- SAP HANA comes with a comprehensive security framework for **secure data access and applications**, with functions for authentication and user management, authorization, masking, anonymization, encryption and auditing.



- SAP HANA is designed to be **set up and run securely** in different environments. Tools, settings, and information help customers to configure, manage and monitor SAP HANA security in their specific environment. SAP HANA cockpit provides a role-based security dashboard, security configuration screens as well as user and role management screens. SAP HANA can be seamlessly integrated into data center security infrastructures via open and documented interfaces.
- Developing **secure software** that is resilient against attack is one of the cornerstones of the SAP security strategy. The secure software development lifecycle process serves as the basis for all development at SAP including SAP HANA.

The purpose of this whitepaper is to give IT security experts an 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 confidentiality, integrity and availability of the data within from common threats like unauthorized access. The whitepaper provides information on

- The different SAP HANA scenarios and their impact on the security approach
- SAP HANA's security framework and functions to secure data and applications
- Secure setup and tools for SAP HANA security configuration, management and monitoring
- SAP's secure software development process and security patch strategy

For further information please also visit our SAP HANA security website at [sap.com/hanasecurity](https://sap.com/hanasecurity).

## WHAT IS SAP HANA?

SAP HANA is the business data platform for the intelligent enterprise. It provides state-of-the-art database and data management technology, advanced analytical capabilities and intuitive application development tools. SAP HANA is available for a wide range of deployment scenarios, both on premises and in the cloud.

SAP HANA can act as a standard SQL-based relational database, for example as data provider for classical transactional applications (OLTP), and/or as data source for analytical requests (OLAP). In addition to standard relational data processing, SAP HANA also provides services to store and process different types of structured and unstructured data (e.g. geo-spatial, graph, text) and supports advanced capabilities such as predictive analytics and machine learning. SAP HANA also integrates seamlessly with other data stores and supports federation and streaming.

SAP HANA is also an application platform that supports a broad variety of programming languages and comes with a comprehensive application development framework and tooling to serve data analysts as well as application programmers.

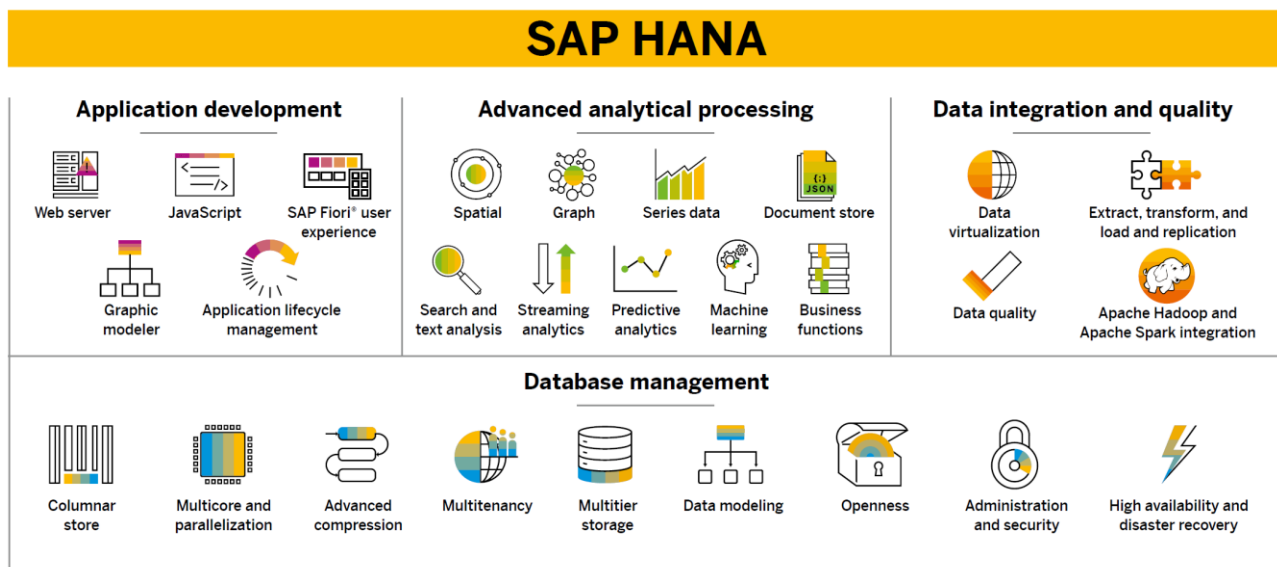


Figure 1: SAP HANA – the platform for the intelligent enterprise

A comprehensive set of security capabilities is provided that allows you to address security and regulatory requirements in different scenarios and deployment environments. SAP HANA security goes beyond the database layer and applies across all different data engines as well as on the integrated application server. SAP HANA can also act as a security federation layer and control access to data across federated data sources.

In the following sections, we give an overview of key SAP HANA security capabilities. For more detailed information, please visit the SAP HANA security website at [sap.com/hanasecurity](https://sap.com/hanasecurity) or see the references at the end of this document.

## Availability

SAP HANA provides comprehensive fault recovery mechanisms, for example service auto-restarts and host auto-failover in scale-out systems. Even though SAP HANA holds the bulk of its data in memory for maximum performance, it still uses persistent storage to provide a fallback in case of failure. After a power outage, SAP HANA can be restarted like any disk-based database and returns to its last consistent state.

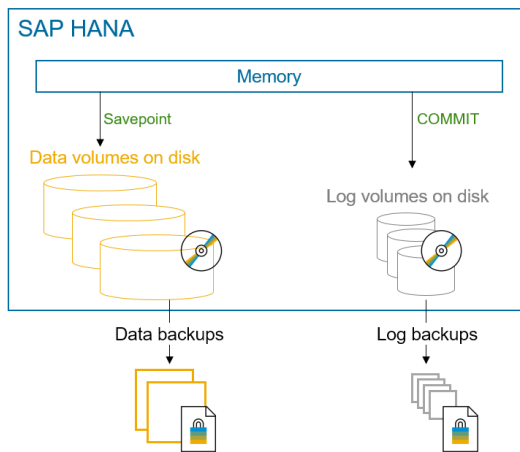


Figure 2: Backup

In addition to traditional data and log backups, SAP HANA provides high-availability and advanced disaster recovery options like storage replication and system replication, which continuously updates secondary systems from a primary system and leverages performance optimizations such as in-memory table loading. Active/active read enabled mode enables the usage of secondary systems for analytics.

## Deployment options

### On-premise deployments

This guide focuses on the on-premise SAP HANA deployment, with the plans to release a technical whitepaper dedicated to the SAP HANA Cloud deployment.

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 are a wide range of cloud deployment options available for SAP HANA. It is available as a managed cloud service (SAP HANA Cloud), can be deployed by customers onto certified cloud infrastructure configurations, and is available as part of a managed application hosting environment. It is also possible to use SAP HANA, express edition for free (32GB memory) in AWS, Azure, or Google Cloud, with the possibility of purchasing a subscription for capacity increases on the [SAP Store](#). Note that feature availability may vary by deployment option.

### Cloud deployments

SAP launched SAP HANA Cloud on March 27<sup>th</sup>, 2020, and with it, the newest offering of a managed SAP HANA cloud service provisioned via the SAP Cloud Platform with multi-cloud deployment options for maximum flexibility.

SAP HANA Cloud is optimized for the cloud, offering one virtual interactive access layer across all data sources with a scalable query engine and data consumption that is decoupled from data management. At the same time, SAP HANA Cloud eases the journey from on-premise deployments to the cloud by providing the ability to run hybrid scenarios and allowing for a gradual migration into the cloud.

The most important difference between the two deployment models lies in the distribution of administration and management responsibilities. On premises, the customer is responsible for setting up and operating the whole hardware and software stack, even though customers might opt for a model where some of these tasks are outsourced to a hardware vendor. When using SAP HANA Cloud, SAP is responsible for setting up and operating the service (as a managed cloud service). Customers choose their configuration options via self-services or service requests and are themselves only responsible for the data layer.

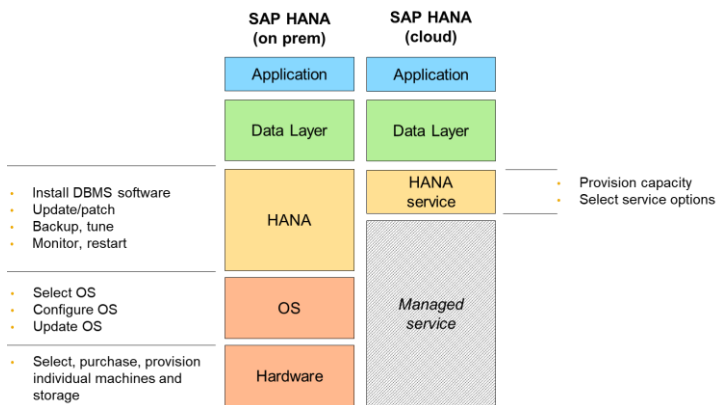


Figure 3: SAP HANA as a managed service

For security this means that the customer configures and controls all options related to data security: users, authentication, roles/authorization, masking, anonymization, auditing. SAP is responsible for the secure setup and secure operations of the system and the whole infrastructure, which includes among other things: data-at-rest encryption and backup encryption, system auditing.

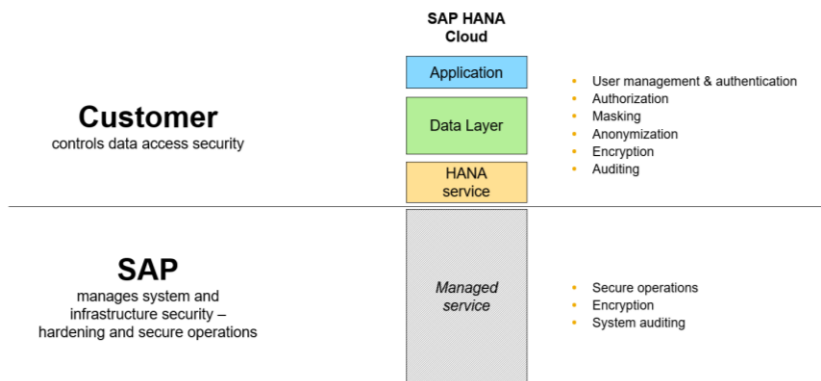


Figure 4: SAP HANA Cloud: Shared responsibility for security

## SCENARIOS DETERMINE THE SECURITY APPROACH

SAP HANA is used in many different scenarios – as a database in SAP Business Warehouse (SAP BW), BW/4HANA, S/4HANA, and SAP Business Suite, for reporting and analytics in data-mart scenarios, and as an application platform. This section will briefly introduce the different scenarios in which SAP HANA can be deployed, how they differ from traditional security approaches, and what customers need to consider from a security perspective when planning their SAP HANA projects.

### SAP HANA as a database in 3-tier scenarios

SAP HANA can be used as a relational database in a classical three-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 or SAP Business Suite. SAP HANA also is the database underneath S/4HANA and BW/4HANA. In those cases, applications are optimized to fully leverage SAP HANA capabilities (e.g. by executing data intensive operations in SAP HANA), but the general 3-tier architecture stays the same.

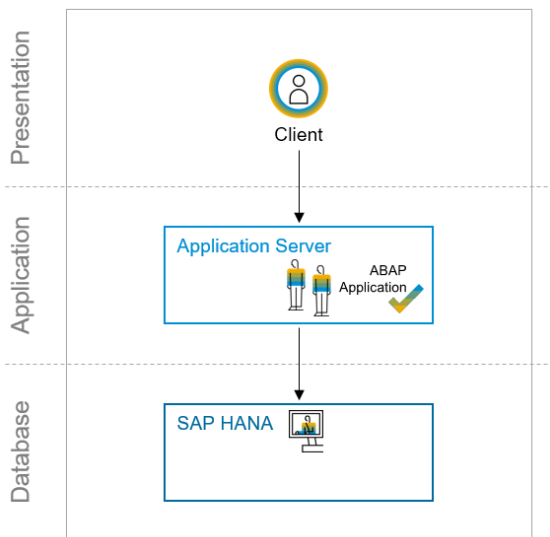


Figure 5: SAP HANA as a database

Using SAP HANA as a database in such scenarios does not change the traditional security model. Security features such as end user authentication, authorization, user management, encryption, and auditing are provided and enforced in the application server layer, while SAP HANA is mainly used as a data store or engine to execute data-intensive operations to maximize performance gains.

The application server connects to SAP HANA through a technical user account. Direct access to SAP HANA is only possible for database administrators, while 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.

### Data marts: customer-specific analytic reporting

Many typical SAP HANA use cases focus on analytic reporting. In these scenarios, data is usually either replicated from a source system such as SAP Business Suite into SAP HANA, or data sources are connected via the federation capabilities of 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 “Secure data and applications”.

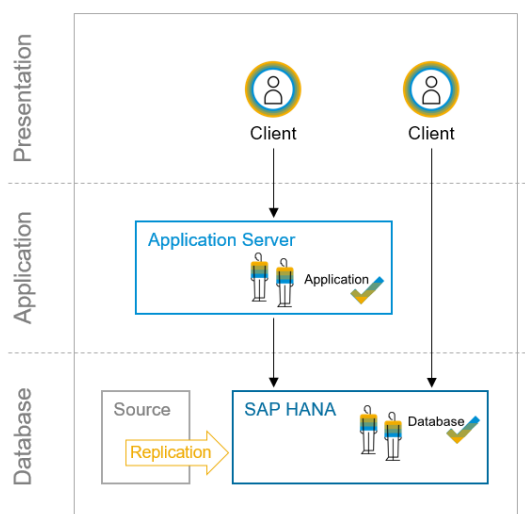


Figure 6: Data mart



## Integrated scenarios

Data that is initially used in the SAP application layer can be made available for analytics directly in SAP HANA to fully leverage its modeling and analytic capabilities. SAP offers integrated support for maintaining matching authorizations, see also “Shared SAP business application authorizations”.

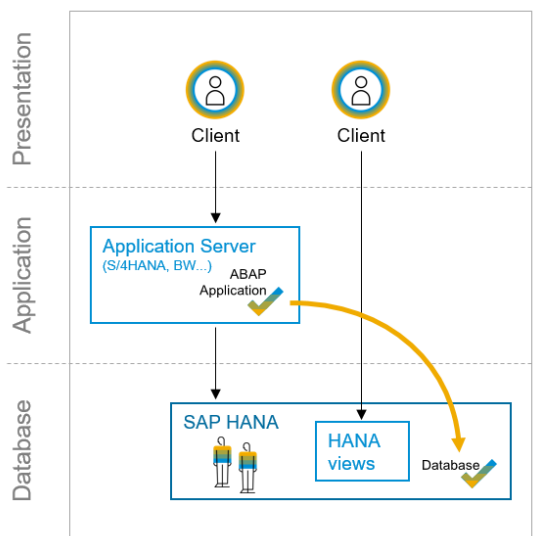


Figure 7: Integrated scenarios

## Application development

**SAP HANA extended application services, advanced model (XS Advanced)** is the default framework for native application development on SAP HANA. It supports a broad variety of programming languages, such as SQLScript for execution on the data layer or Java and node.js for execution in the application server runtime. End user clients access applications developed on XS Advanced via HTTP(S), while the application runtimes communicate with the SAP HANA database via SQL. XS Advanced provides deployment flexibility and specific security options.

Application and database layer can be decoupled. You can either install XS Advanced directly on the SAP HANA server or install it on a host that is separate from the SAP HANA database. This enables you to scale XS Advanced independently of the database, as you can have many more XS Advanced nodes than SAP HANA database nodes. You can also install XS Advanced in a separate network from SAP HANA itself, which makes it possible to put XS Advanced applications into a different network zone and have a firewall between the application and database layers. Applications are strictly isolated from each other. They are deployed in dedicated containers via the SAP HANA deployment infrastructure (HDI) on the database layer. On the application layer, you can use dedicated operation system users per application.

XS Advanced business users are managed via an identity provider, either using external SAML2-compliant identity provider or SAP HANA as native identity provider. Authentication is handled by a central user account and authentication server (UAA). XS Advanced business users are authorized based on XS Advanced scopes and attributes. User-specific authorizations can be enforced on the application and the database layer (row level). SAP Web IDE for SAP HANA is used for application development. For application source code management, integration with GIT is available.



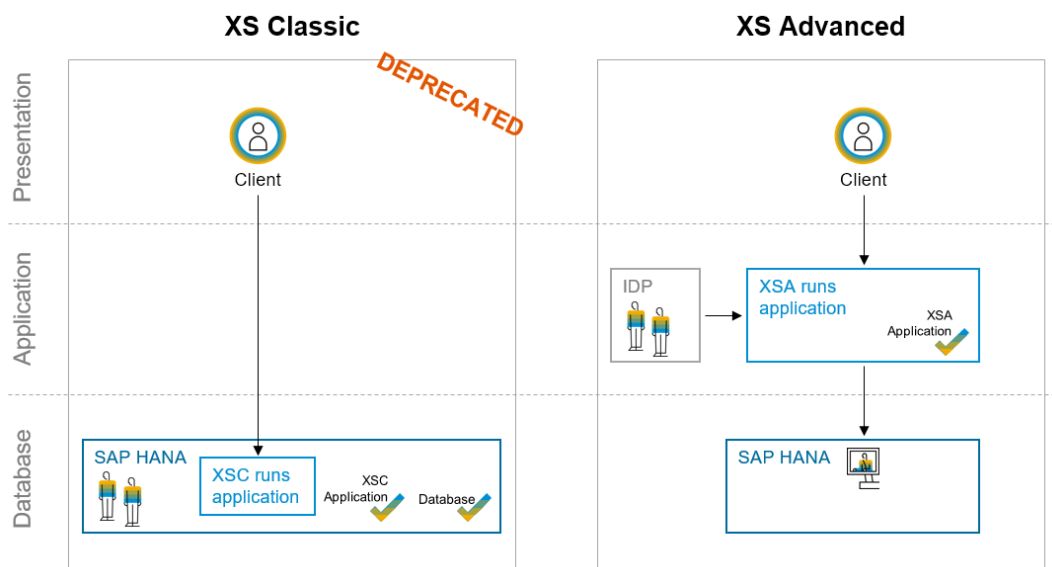


Figure 8: SAP HANA as application platform

The **SAP HANA extended application services, classic model (XS Classic)** application development framework was introduced in earlier versions of SAP HANA. Even though it is still available today, it has been deprecated and SAP plans to remove it in a future SAP HANA release (see SAP Note 2465027). SAP recommends customers to plan the transition of existing content and applications to XS Advanced and use XS Advanced for new application development.

XS Classic embeds a full-featured application server, web server and development environment within SAP HANA itself. Applications can be deployed directly on SAP HANA and can be accessed by end users via HTTP(S). As XS Classic is part of SAP HANA, the same security model applies. This means that the majority of security features described in the section “Shared SAP business application authorizations” apply directly to such XS applications. Additionally, support for protection against typical vulnerabilities of web-based applications, for example XSRF, is available.

## SECURE DATA AND APPLICATIONS

SAP HANA is designed to run securely in different scenarios and deployment modes. The security framework enables customers to implement security policies and compliance requirements for their specific SAP HANA scenario.

This section provides an overview of SAP HANA’s security functions and how they can be used to manage and control compliant access to data. Depending on the scenario in which SAP HANA is used (see “Scenarios determine the security approach”), only some of these SAP HANA security functions might actually be needed, while others might be provided by different architecture layers. Detailed information on the available security functions can be found in the SAP HANA Security Guide.

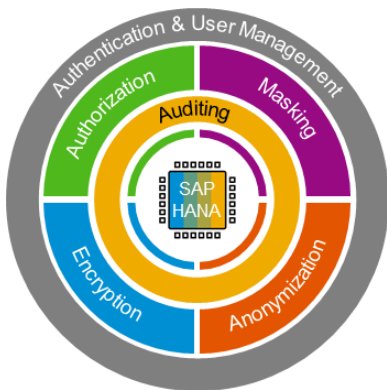


Figure 9: SAP HANA security framework

## User and identity management

For direct logon to SAP HANA, a user in SAP HANA is required. Depending on the scenario, this user can either be a technical account, a database administrator, or an individual end user. For user management, you can use SAP HANA cockpit, SAP HANA's administration tool. You can also configure automatic user provisioning based on LDAP, leveraging user information that you keep in a central LDAP directory and thus significantly reducing cost of maintenance. Adapters are available for SAP Identity Management and SAP Access Control, which allow integration into existing user provisioning infrastructures. To connect custom user provisioning solutions, SAP HANA's SQL interface can be leveraged.

User groups allow you to manage related users together and to assign security policies. The following scenarios are currently supported: dedicated group user administrators can be created to manage individual user groups and implement a separation of duties (SoD) for user management tasks, and user-group-specific security policies can be defined. Note that user groups don't control data access: roles and privileges are SAP HANA's mechanism for managing data access, see "Authorization and role management".

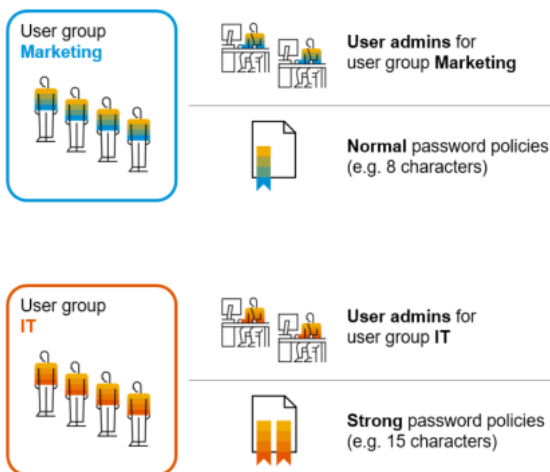


Figure 10: Example for different user groups

## 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 customizable password policy governs change frequency, password complexity and other password-related security settings. SAP HANA does not use any default passwords. After first logon, users are forced to set new passwords. SAP HANA also supports authentication against an LDAP server. In addition, several single sign-on methods are available.

**Authentication**

**Edit**

**Password Policy** | Password Blacklist

| Password Length and Composition    | Password Lifetime                                |
|------------------------------------|--|
| Minimum Number of Characters:<br>8 | Lifetime of Initial Password:<br>7 days          |
| Lowercase Letters Required:<br>1   | Minimum Password Lifetime:<br>1 day              |
| Uppercase Letters Required:<br>1   | Maximum Password Lifetime:<br>182 days           |
| Numerical Digits Required:<br>1    | Maximum Duration of User Inactivity:<br>365 days |
| Special Characters Required:<br>0  | Notification of Password Expiration:<br>14 days  |

| User Lock Settings                        | Miscellaneous   |
|---|---|
| User Lock Time:<br>1,440 minutes          | Number of Allowed Failed Logon Attempts:<br>6             |
| SYSTEM User Is Exempt from Locking:<br>No | Number of Last Used Passwords That Cannot Be Reused:<br>5 |
|   | Password Change Required on First Logon:<br>Yes           |
|   | Detailed Error Information on Failed Logon:<br>No         |

Figure 11: Password policy configuration in SAP HANA cockpit

| Single sign-on method | SAP HANA<br>JDBC/ODBC | XS Classic<br>HTTP(S) | XS Advanced<br>HTTP(S) |
|-----------------------|-----------------------|-----------------------|------------------------|
| Kerberos/SPNego       | yes                   | yes                   | yes                    |
| SAML                  | yes                   | yes                   | yes                    |
| SAP Logon Tickets     | yes                   | yes                   | no                     |
| SAP Assertion Tickets | yes                   | yes                   | no                     |
| JWT                   | yes                   | no                    | yes                    |
| X.509                 | no                    | yes                   | yes                    |

## Authorization and role management

SAP HANA's authorization framework provides highly granular data access control. The actions that a user can perform depend on the assigned roles and privileges. Roles are used to bundle and structure privileges for users. Role design and role assignment to end users can be separated (role transport from development to production system). Note that in XS Advanced applications, business end users are authorized in the XS Advanced layer (no need for SAP HANA roles).

Note: SAP recommends customers to plan the migration of existing repository roles to HDI-based roles (HDI = HANA deployment infrastructure) and use HDI-based roles for projects, as the repository is deprecated (see SAP Note 2465027). A best practice guide for the migration and HDI role development is available.

LDAP groups can be leveraged for automatically assigning roles to users in SAP HANA. Using an LDAP server as a central repository for authorizations significantly reduces complexity for maintaining authorizations in large system landscapes.

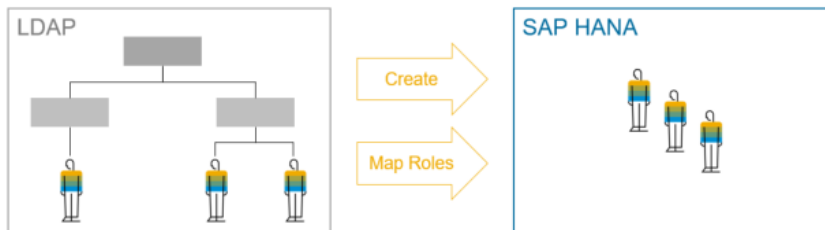


Figure 12: LDAP integration

Privileges define what users can see and do in SAP HANA: “no privilege” means “no access”. SAP HANA privileges are based on standard SQL privileges, with SAP HANA-specific extensions for business applications. SQL (object) privileges authorize access to data and operations on database objects (tables, views, procedures etc.), while analytic privileges provide fine-granular access control on the row level.

Database administrators in SAP HANA do not automatically have access to the content (data) of schemas and views. They need to be granted the relevant SQL privileges like any other end user in SAP HANA. There is a specific set of privileges (“system privileges”) for authorizing the execution of database administration tasks such as backup or user management.

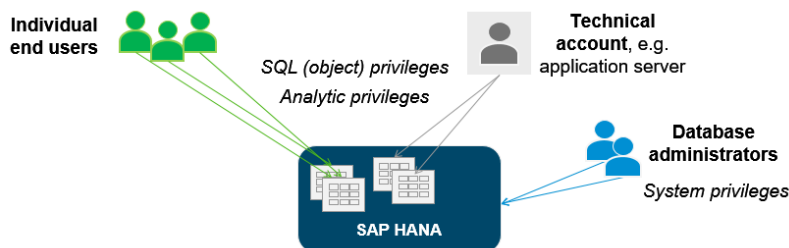


Figure 13: Privilege types

Applications running on XS Advanced use their own authorization concept in the XS Advanced layer. For applications running on XS Classic additional application privileges are available, which apply on top of the usual SAP HANA privileges.

### Shared SAP business application authorizations

The basic layer of authorization for ABAP-based SAP applications such as S/4HANA is provided by “authorization objects” in the SAP NetWeaver Application Server for ABAP. It is possible to create analytic privileges in SAP HANA that reuse these authorizations for read access. When you reuse ABAP authorization objects in SAP HANA, access to views in SAP HANA is based on the authorizations as they are maintained in the ABAP system. This means that the names of the database user in SAP HANA executing the query and the name of the user on the ABAP server have to match.

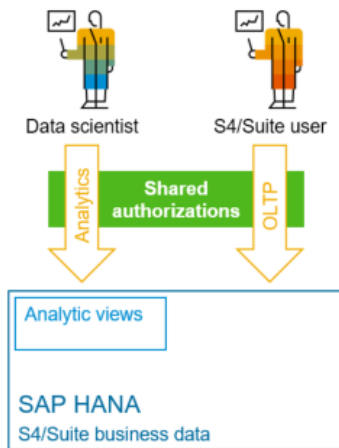


Figure 14: Shared SAP business application authorizations

Being able to create analytic privileges based on ABAP authorizations means that you can provide consistent access to your SAP business data from both SAP applications and new applications built using the SAP HANA extended application services, advanced model. It also reduces the effort of maintaining your authorization model.

## Masking

Masking obfuscates parts of the data in columns, or completely substitutes the cleartext data with synthetic data. Typical use cases are for example to hide sensitive information from DBAs and other power users with broad access rights, or to display/hide sensitive information depending on the user role for example in a call center.

| CREDIT_CARD_NO     | NAME            | BALANCE |
|--------------------|-----------------|---------|
| XXXX-XXXX-XXXX-005 | Julie Armstrong | ***     |
| XXXX-XXXX-XXXX-431 | Michael Adams   | ***     |
| XXXX-XXXX-XXXX-000 | Richard Wilson  | ***     |
| XXXX-XXXX-XXXX-188 | Nathalie Perrin | ***     |

Figure 15: Dynamic data masking

SAP HANA supports dynamic data masking i.e. it is applied when the data is queried, while the original data remains unchanged and can continue to be used for other purposes and use cases. Mask expressions can be defined on views and on tables. Mask expressions are fully customizable and can use constants, built-in and as well as user-defined functions. Masking is completely integrated into SAP HANA's authorization framework: only users with the UNMASKED privilege on the relevant table or view can see cleartext data. Note that no user in SAP HANA has this privilege by default.

## Data anonymization

While data masking is a very important tool for many use cases that need to hide parts of sensitive records, it is often not suitable for protecting complex mass data. Common pitfalls include that masking does not always achieve the required level of security or that the masked data is stripped of too much information and can no longer be used for the intended purpose. Data anonymization provides a structured approach to protect sensitive data while still preserving the ability to use it in defined analytic scenarios. It lets you gain insights from data that could not be leveraged before due to regulations.

Similar to masking, data anonymization is applied when data is queried, leaving the original data unchanged.

SAP HANA supports the following anonymization methods, which are also proposed in the *EU Opinion 05/2014 on Anonymization Techniques*:

- k-anonymity, which hides individuals in a larger set of data records
- Differential privacy, which applies statistical noise to hide sensitive values

| Name   | Birth   | City    | Weight | Illness            |
|--------|---------|---------|--------|--------------------|
| Paul   | 07-1975 | Waldorf | 82 kg  | AIDS               |
| Martin | 10-1975 | Hamburg | 110 kg | Lung Cancer        |
| Nils   | 01-1975 | Munich  | 70 kg  | Flu                |
| Annika | 09-1987 | Berlin  | 58 kg  | Multiple Sclerosis |



*Medical researcher: Link between weight and cancer?*

| Name        | Birth             | Location | Weight  | Illness            |
|-------------|-------------------|----------|---------|--------------------|
| 0c4a67      | 1975              | Germany  | ~ 96 kg | AIDS               |
| df89aa      | 1975              | Germany  | ~ 96 kg | Lung Cancer        |
| 305be2      | 19**              | Germany  | ~ 64 kg | Flu                |
| 7422c2      | 19**              | Germany  | ~ 64 kg | Multiple Sclerosis |
| Identifiers | Quasi-identifiers |          |         | Sensitive          |

Figure 16: k-anonymity example

Data anonymization methods and parameters are defined in customizable anonymization views, allowing for maximum flexibility and transparency. Data scientists can use SAP Web IDE to configure anonymization scenarios. Additionally, there is a dedicated view available for data protection officers, who usually also are involved in projects with personal data and need suitable information in order to approve such scenarios. Data anonymization is completely integrated into SAP HANA's security framework: you can control the access to anonymization views via privileges, and track who accessed the anonymized data using audit logging.

## Encryption

While authorization is the primary means for access control, encryption provides an additional layer of protection. SAP HANA provides comprehensive encryption capabilities both for data at rest and in motion. SAP HANA encryption is based on SAP's standard cryptographic library, which is certified for FIPS 140-2.

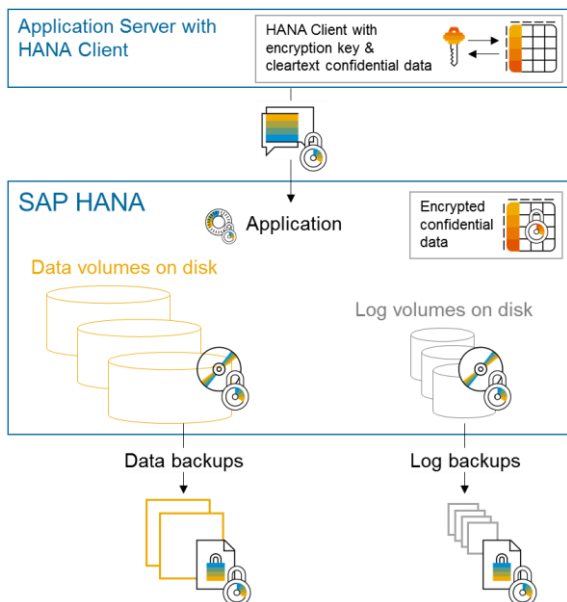


Figure 17: Encryption overview

## Backup encryption

Backup encryption prevents unauthorized parties from reading the content of backups. Backups written to the file system and to 3<sup>rd</sup> party backup tools via the Backint interface can be encrypted using the AES-256-CBC algorithm. If you are using a 3<sup>rd</sup>-party backup tool, you have a choice between native SAP HANA encryption or tool-side backup encryption. Complete data backups, delta data backups, and log backups can be encrypted. The encryption of backups is independent of the data volume and redo log encryption.

## Data and log encryption

SAP HANA uses persistent storage (data files) to provide a fallback in case of failure. Data is automatically saved from memory to data files on disk at regular savepoints. Additionally, all data changes are captured in redo log entries that are written to disk with each committed database transaction (redo log files). Data and redo log files on disk can be encrypted using the AES-256-CBC algorithm. Note that encryption does not increase the file size on disk.

## Column encryption

Column encryption provides a fine-granular encryption option for table columns. The encryption keys are controlled by the client driver: it collaborates with the SAP HANA server to encrypt/decrypt column data on the client side. The SAP HANA server has no access to cleartext data or cleartext keys. This means that the data on the server side will always be encrypted, both on disk and in-memory.

## Application encryption

Encryption APIs are available for applications based on SAP HANA extended application services (XS) for storing values in encrypted form. SAP HANA's internal application encryption service takes care of the encryption key handling so that encryption keys are never directly accessed by the application or an application user. When implementing encryption for an XS application, application developers can decide whether the encrypted data should be accessible application-wide (all users of the application can access the decrypted data), or per application user. Application-wide encryption could be used, for example, for a password that the application needs to access a remote service. User-specific encryption could be used for PIN codes or credit card numbers.

## Encryption configuration and key management

You can switch on encryption with the click of a button in SAP HANA cockpit, the web-based administration tool for SAP HANA.

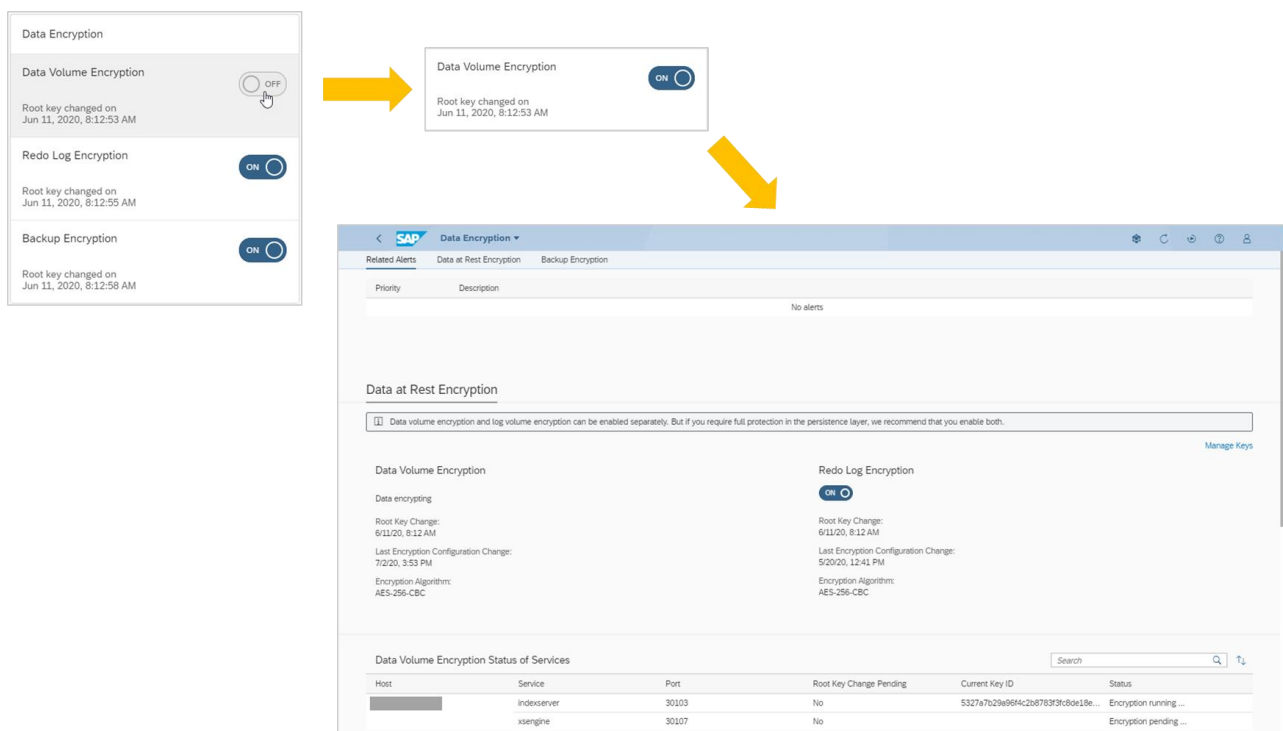


Figure 18: Encryption configuration in SAP HANA cockpit

SAP HANA uses SAP's secure store in the file system (SSFS) to protect all encryption root keys. Encryption keys are unique and can be changed depending on customers' key rotation requirements. Detailed information on encryption keys is available in SAP HANA cockpit, and you can easily manage the lifecycle of your encryption keys using SAP HANA cockpit's functions for key backup and key change.

It is also possible to use a key server to control access to the SAP HANA data encryption keys. SAP HANA local secure store (LSS) is leveraged to connect to SAP Data Custodian key management service as the first supported key server. LSS is a separate, lightweight utility for storing and securely managing the HANA encryption root keys, which is part of the SAP HANA installation. It allows a stronger separation between system administration and encryption key management. SAP Data Custodian KMS is a cloud product which is available as SaaS through a monthly or annual subscription. It supports customer-controlled keys and uses a FIPS 140-2 Level 3 compliant key vault. It is possible to import a key from your preferred HSM into Data Custodian KMS or you can generate the key with Data Custodian.



Note: The management of column encryption keys requires configuration both on the SAP HANA server and the client side. It has not been included yet in SAP HANA cockpit.

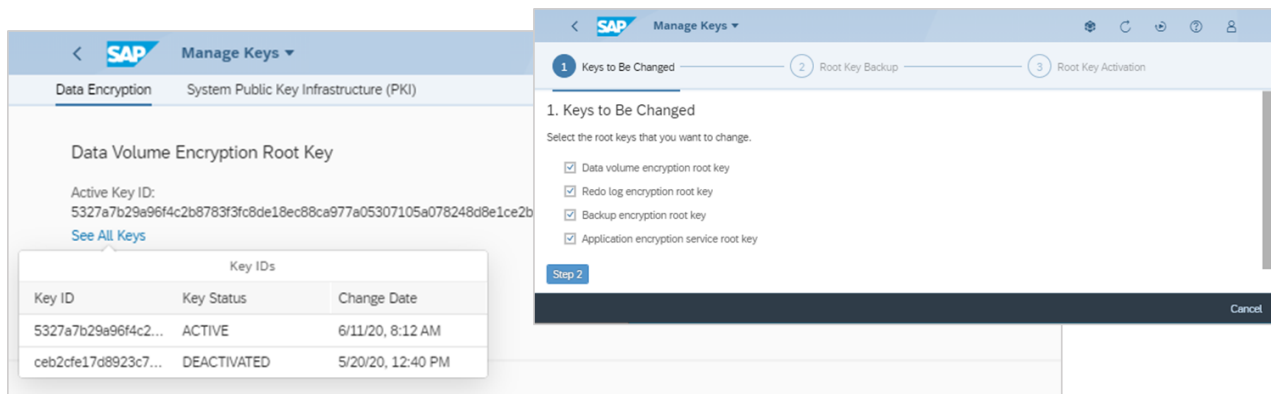


Figure 19: Key management in SAP HANA cockpit

### Communication encryption: TLS/SSL

SAP HANA supports TLS/SSL connection encryption for network communication channels. Encryption of client-server communication (external channels) can be enforced. Server certificates needed for TLS/SSL client-server communication over JDBC/ODBC can be stored directly in SAP HANA and configured using SAP HANA cockpit, thus simplifying certificate management considerably.

All internal SAP HANA communication can be secured using TLS/SSL. A public-key infrastructure (PKI) is automatically set up during installation for this purpose.

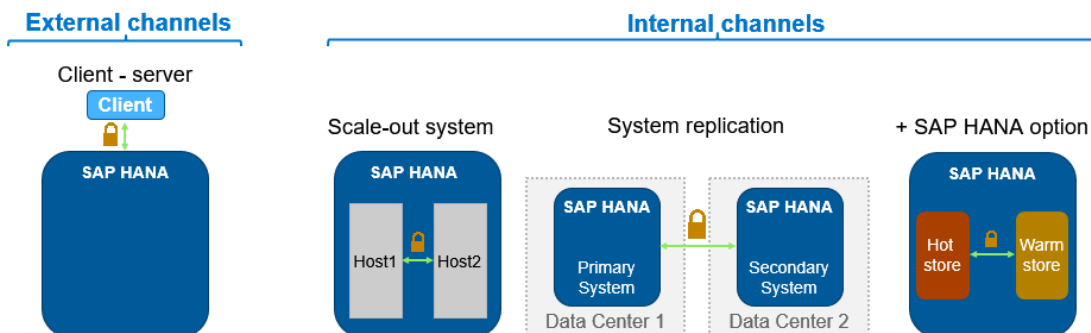


Figure 20: Secured communication channels in SAP HANA

A best practice guide for configuring TLS/SSL in typical SAP HANA scenarios is available.

### Auditing

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 be written to Linux syslog and/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.

You can use SAP HANA cockpit to view and filter the audit trail, as well as to set audit retention policies.


| Audit Policies Configuration Audit Trail   |                      |          |            |             |              |  |
|--|----------------------|----------|------------|-------------|--------------|--|
| Log Entries (15)   |                      |          |            |             |              |  |
| Delete Audit Entries  |                      |          |            |             |              |  |
| Time Stamp   | Policy Name          | Level    | Status     | Client Host | User Name    | Statement  |
| 2020-07-02 21:10:04  | CriticalAccess       | CRITICAL | SUCCESSFUL |             | AUDITOR      | SELECT * FROM SYSTEM.ACCOUNTS  |
| 2020-07-02 21:09:58  | CriticalAccess       | CRITICAL | SUCCESSFUL |             | BUSINESSUSER | SELECT * FROM SYSTEM.ACCOUNTS  |
| 2020-07-02 21:09:58  | CriticalAccess       | CRITICAL | SUCCESSFUL |             | BUSINESSUSER | SELECT * FROM SYSTEM.ACCOUNTS  |
| 2020-07-02 21:09:58  | MandatoryAuditPolicy | CRITICAL | SUCCESSFUL |             | SYSTEM       | CREATE AUDIT POLICY "CriticalAccess" AUDITING ALL INSERT, SELECT, UPDATE ON "SYSTEM"."ACCOUNTS" LEVEL CRITICAL |
| 2020-07-02 21:09:58  | MandatoryAuditPolicy | CRITICAL | SUCCESSFUL |             | SYSTEM       | CREATE AUDIT POLICY "CriticalAccess" AUDITING ALL INSERT, SELECT, UPDATE ON "SYSTEM"."ACCOUNTS" LEVEL CRITICAL |
| 2020-07-02 21:09:58  | MandatoryAuditPolicy | CRITICAL | SUCCESSFUL |             | SYSTEM       | ALTER AUDIT POLICY firefighter_dev DISABLE   |

Figure 21: Audit trail analysis in SAP HANA cockpit

## SECURE SETUP

SAP HANA is designed to run securely in different environments and provides “security by default”<sup>1</sup> for example with the default multi-tenancy mode. As incorrect security settings are one of the most common causes of security problems, SAP offers information and tools that help you run your SAP HANA system securely.

### Default multi-tenancy mode

SAP HANA has built-in multi-tenancy support, and all systems since SAP HANA 2.0 SPS 01 are automatically set up in multi-tenancy mode. Systems can easily be extended by adding new tenant databases, and multi-tenancy helps you to simplify database management and lower TCO.

An SAP HANA system consists of a system database for system administration tasks, and one or more tenant databases for the actual data management. All databases in an SAP HANA system share the same installation of database system software and the same computing resources. However, each database is self-contained and fully isolated with its own set of database users, database catalog, persistence, backups, traces and logs, and workload management. Database clients, such as the SAP HANA cockpit, connect to specific databases.

Security benefits of multi-tenancy include a stronger protection of application data through the isolation in dedicated tenant databases, additional options for a segregation of duties with separate administration for system and tenant databases, separate networks for system administration and application access, and an overall system administration from system database that cannot access tenant content. Tenant databases can be hardened individually (e.g. TLS/SSL, encryption), and it is possible to restrict per tenant which administration functions are available. A special high-isolation mode provides even stronger isolation including separate operating system users.

<sup>1</sup> “secure by default” refers to the most secure software settings being configured or activated by default

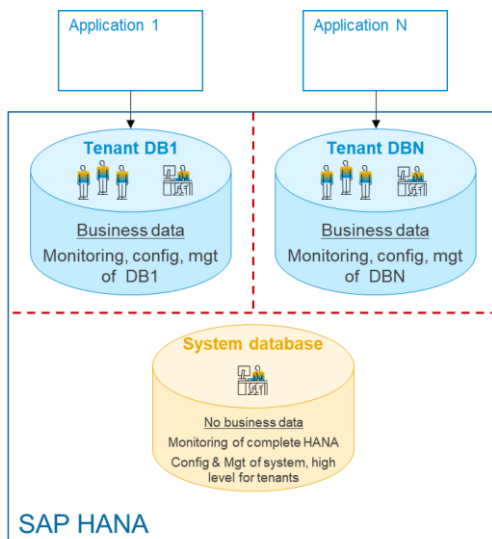


Figure 22: Multitenancy: two levels of administration

## Security information

The comprehensive SAP HANA security guide provides in-depth information on the SAP HANA security concepts and functions including information on data protection and privacy. The SAP HANA security checklists, which are also integrated in the SAP HANA cockpit, provide hands-on information for configuring and validating the most critical security settings.

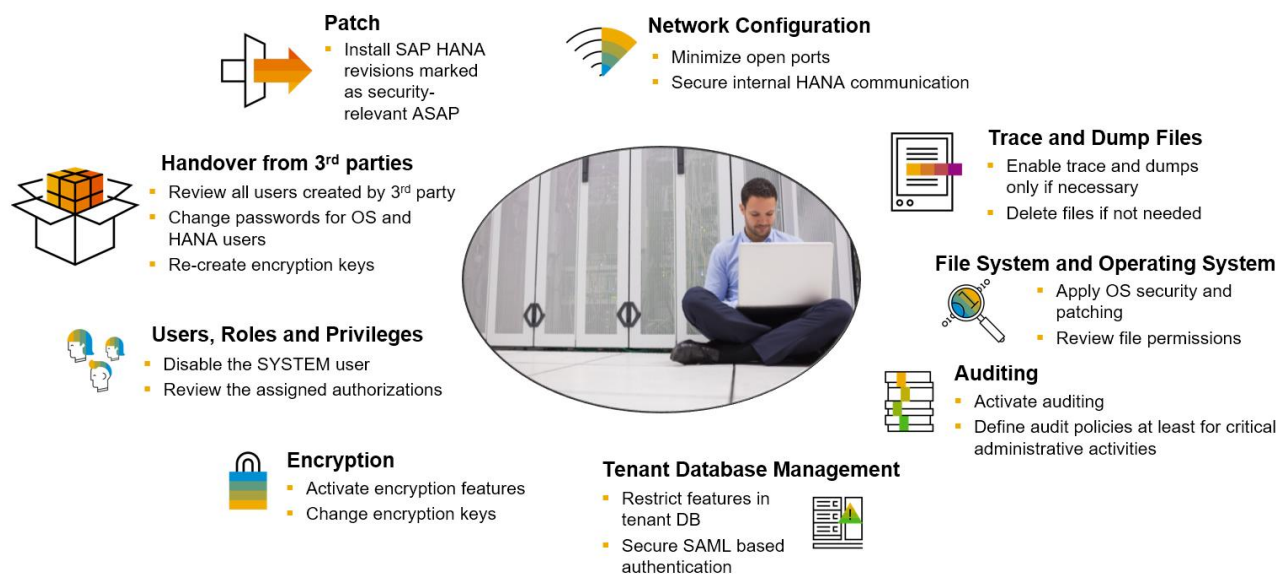


Figure 23: Security checklists

## Tools for security configuration, management and monitoring

SAP HANA's main administration tool is the web-based SAP HANA cockpit, which is also used for security configuration, management and monitoring of SAP HANA system landscapes as well as of individual SAP HANA systems. The legacy SAP HANA studio administration tool is deprecated, see SAP Note 2465027.

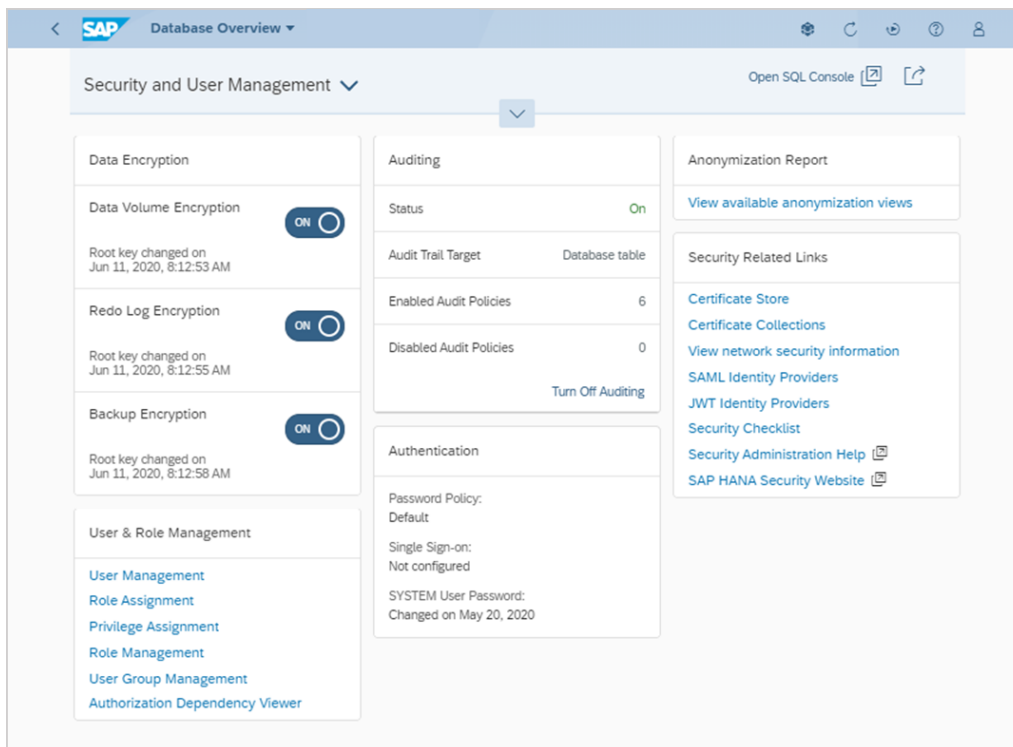


Figure 24: Security management in SAP HANA cockpit

SAP HANA is also integrated into standard SAP tools such as SAP Solution Manager and supported by services like SAP Early Watch Alert, Security Optimization Services, System Recommendations and Configuration Validation.

### Interfaces and 3rd party tool support

SAP HANA supports industry standard and documented interfaces to enable a seamless integration with the customers' security network and datacenter infrastructures. Most security administration tasks can also 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 and SAML. For integration into an enterprise logging infrastructure, SAP HANA auditing supports Linux syslog. Antivirus software can be used for XS applications via a dedicated antivirus interface.

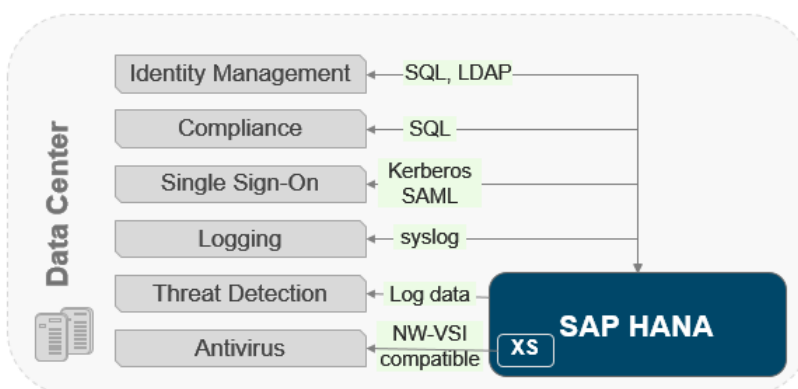


Figure 25: SAP HANA data center integration

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

- [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

## Data protection and privacy

SAP HANA provides the technical enablement and infrastructure to allow you run applications on SAP HANA to conform to the legal requirements of data protection in the different scenarios in which SAP HANA is used. Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy regulations, it is necessary to consider compliance with industry-specific legislation in different countries. SAP HANA provides specific features and functions to support compliance with regard to relevant legal requirements, including data protection.

This section does not give any advice on whether these features and functions are the best method to support company, industry, regional, or country-specific requirements. Furthermore, it does not give any advice or recommendations regarding additional features that would be required in specific IT environments; decisions related to data protection must be made by the customer on a case-by-case basis, taking into consideration the given system landscape and the applicable legal requirements.

Many data protection requirements depend on how the business semantics or context of the data stored and processed in SAP HANA are understood. In SAP HANA installations, the business semantics of data are part of the application definition and implementation. SAP HANA provides the features for working with technical database objects, such as tables. It is therefore the application that "knows", for example, which tables in the database contain sensitive personal data, or how business level objects, such as sales orders, are mapped to technical objects in the database. Applications built on top of SAP HANA need to make use of features provided by SAP HANA to implement compliance requirements for their specific use case.

SAP HANA provides a variety of security-related features to implement general security requirements that are also required for data protection and privacy:

- Access control – Authentication, authorization, data masking and anonymization, data encryption
- Access logging – Auditing
- Transmission control/communication security – Encrypted communication (TLS/SSL)
- Availability control – Backup and recovery, storage and system replication, service auto-start, host auto-failover
- Separation by purpose – Subject to the organization model, must be applied as part of the authorization concept. Isolated storage can be achieved using database schemas and tenant databases.
- Deletion – SQL deletion commands

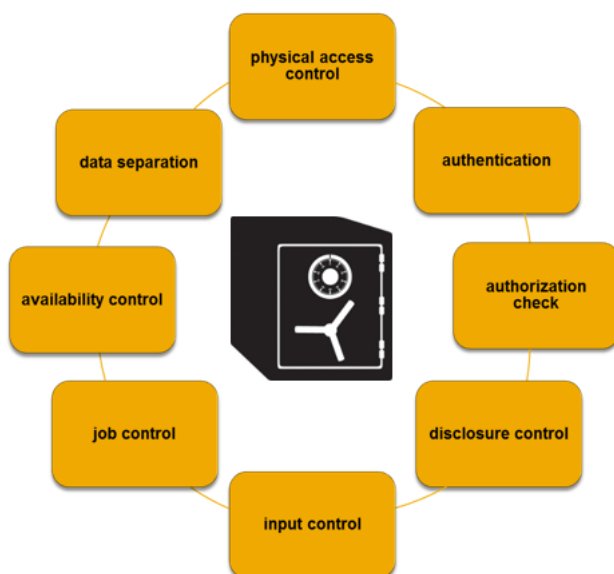


Figure 26: Data protection and privacy

## SECURE SOFTWARE

### Secure development

SAP HANA is developed according to SAP's secure development lifecycle, which is a comprehensive framework of processes, guidelines, tools and staff training to safeguard the architecture, design and implementation of all SAP solutions.

The secure development lifecycle is a threat-based approach, which includes risk and data protection assessments, comprehensive security testing including automated and manual tests and penetration testing, and a separate security validation phase. For more information, see [sap.com/security](https://sap.com/security).

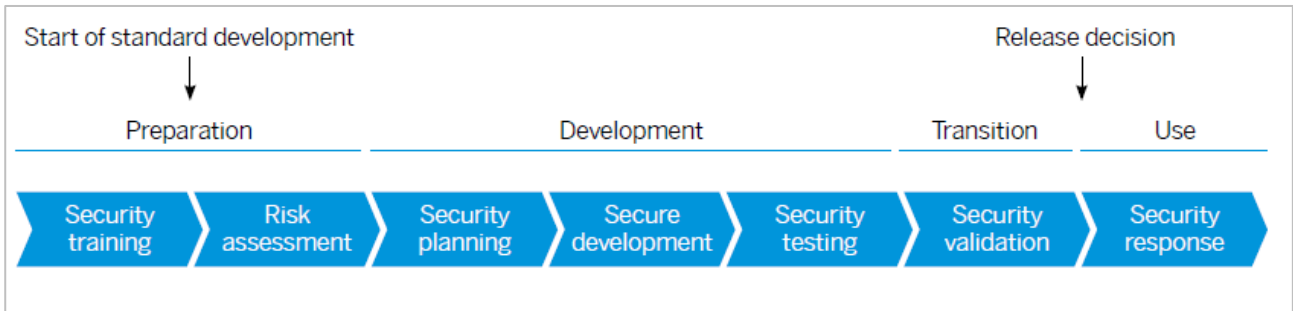


Figure 27: Secure software development lifecycle

### Security patches

SAP HANA is part of SAP's monthly security patch day process. Information about SAP HANA security patches is published in SAP security notes according to SAP's security patch strategy, which provide information on affected components and measures that protect against the exploitation of potential weaknesses.

Security patches are delivered as SAP HANA revisions and can be applied using SAP HANA's lifecycle management tools. SAP HANA provides tools that simplify testing and execution of updates. The capture and replay tool for SAP HANA allows you to test your production workload in a test system. For eliminating/reducing business downtimes, zero downtime maintenance (based on system replication) or upgrade by moving tenants can be used. Operating system patches are provided by the respective operating system vendors.

## FURTHER READING

|                              |  |
|------------------------------|--|
| <b>Website</b>               | <ul style="list-style-type: none"><li>• <a href="http://www.sap.com/hanasecurity">http://www.sap.com/hanasecurity</a></li></ul>  |
| <b>Recent blogs</b>          | <ul style="list-style-type: none"><li>• <a href="#">Expedite your security configuration with SAP HANA 2.0 SPS 05</a></li><li>• <a href="#">Are security concerns keeping you from innovating?</a></li><li>• <a href="#">Anonymization: analyze sensitive data without compromising privacy</a></li></ul>  |
| <b>Anonymization Website</b> | <ul style="list-style-type: none"><li>• <a href="http://www.sap.com/data-anonymization">http://www.sap.com/data-anonymization</a></li></ul>  |
| <b>Documentation</b>         | <ul style="list-style-type: none"><li>• <a href="#">SAP HANA Security Guide</a></li><li>• <a href="#">SAP HANA Security Checklists and Recommendations</a></li><li>• <a href="#">SAP HANA Administration Guide</a></li><li>• <a href="#">SAP HANA SQL and System Views Reference</a></li><li>• <a href="#">SAP HANA SQL Command Network Protocol</a></li></ul> |
| <b>Guides and templates</b>  | <ul style="list-style-type: none"><li>• <a href="#">Developing SAP HANA roles using HDI/XS Advanced</a></li><li>• <a href="#">Configuring TLS/SSL in typical SAP HANA scenarios</a></li><li>• <a href="#">SAP Security Baseline Template (logon required)</a></li></ul>  |
| <b>Training course</b>       | <ul style="list-style-type: none"><li>• <a href="#">HA240: Authorization, Security, and Scenarios (classroom training)</a></li></ul>   |
| <b>Videos</b>                | <ul style="list-style-type: none"><li>• <a href="#">SAP HANA Academy: security playlist on YouTube</a></li></ul>   |
| <b>SAP Notes</b>             | <ul style="list-style-type: none"><li>• <a href="#">SAP Note 2378962 – SAP HANA revision und maintenance strategy (logon required)</a></li><li>• <a href="#">SAP Security Notes</a></li><li>• <a href="#">SAP Note 2465027 – Deprecation of SAP HANA extended application services, classic model and SAP HANA Repository (logon required)</a></li></ul>       |
| <b>SAP security</b>          | <ul style="list-style-type: none"><li>• <a href="http://www.sap.com/security">http://www.sap.com/security</a></li><li>• <a href="#">SAP secure development lifecycle</a></li><li>• <a href="#">FIPS certification of SAP's cryptographic library</a></li></ul>   |
| <b>SAP HANA</b>              | <ul style="list-style-type: none"><li>• <a href="https://www.sap.com/products/hana.html">https://www.sap.com/products/hana.html</a></li><li>• Hasso Plattner, In-Memory Data Management: Technology and Applications (2012)</li></ul>  |
| <b>Miscellaneous</b>         | <ul style="list-style-type: none"><li>• <a href="#">EU Opinion 05/2014 on Anonymization Techniques proposes k-anonymity (and derivatives) and differential privacy</a></li></ul>   |



[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2021 SAP SE or an SAP affiliate company. 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 or an SAP affiliate company.

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. National product specifications may vary.

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 or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP 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, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. See [www.sap.com/trademark](http://www.sap.com/trademark) for additional trademark information and notices.

**THE BEST RUN**

