



# **SAP Skills Forum 2017**

## **SAP HANA Security**

Andrea Kristen, SAP HANA Product Management  
June 2017

PUBLIC





# Agenda

Scenarios determine the security approach

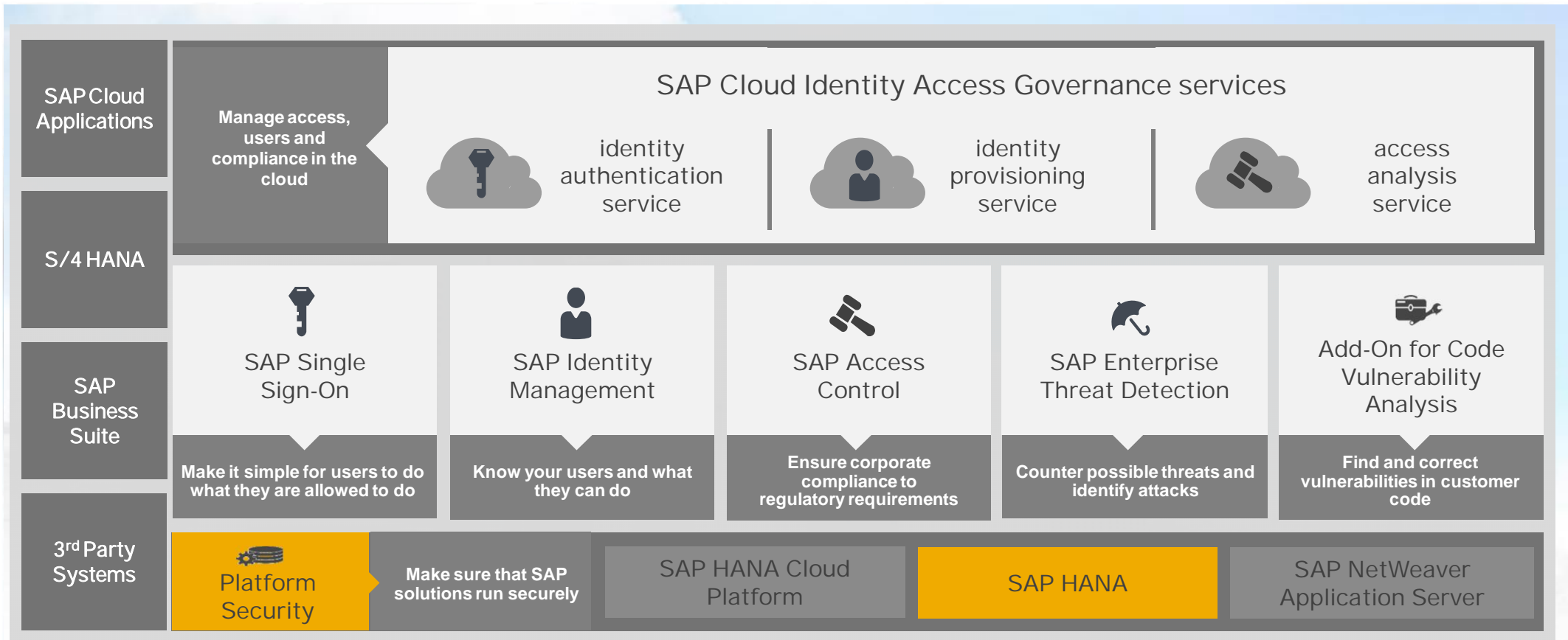
Secure information access

Secure configuration and operations

Recent innovations and roadmap

Secure software, release strategy and patching

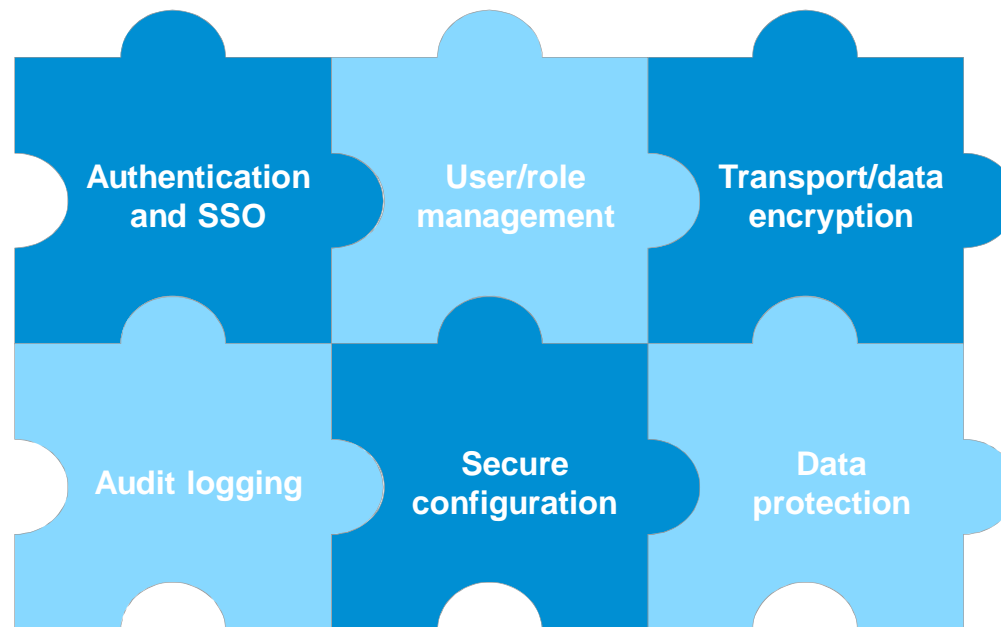
# SAP security and GRC access governance portfolio



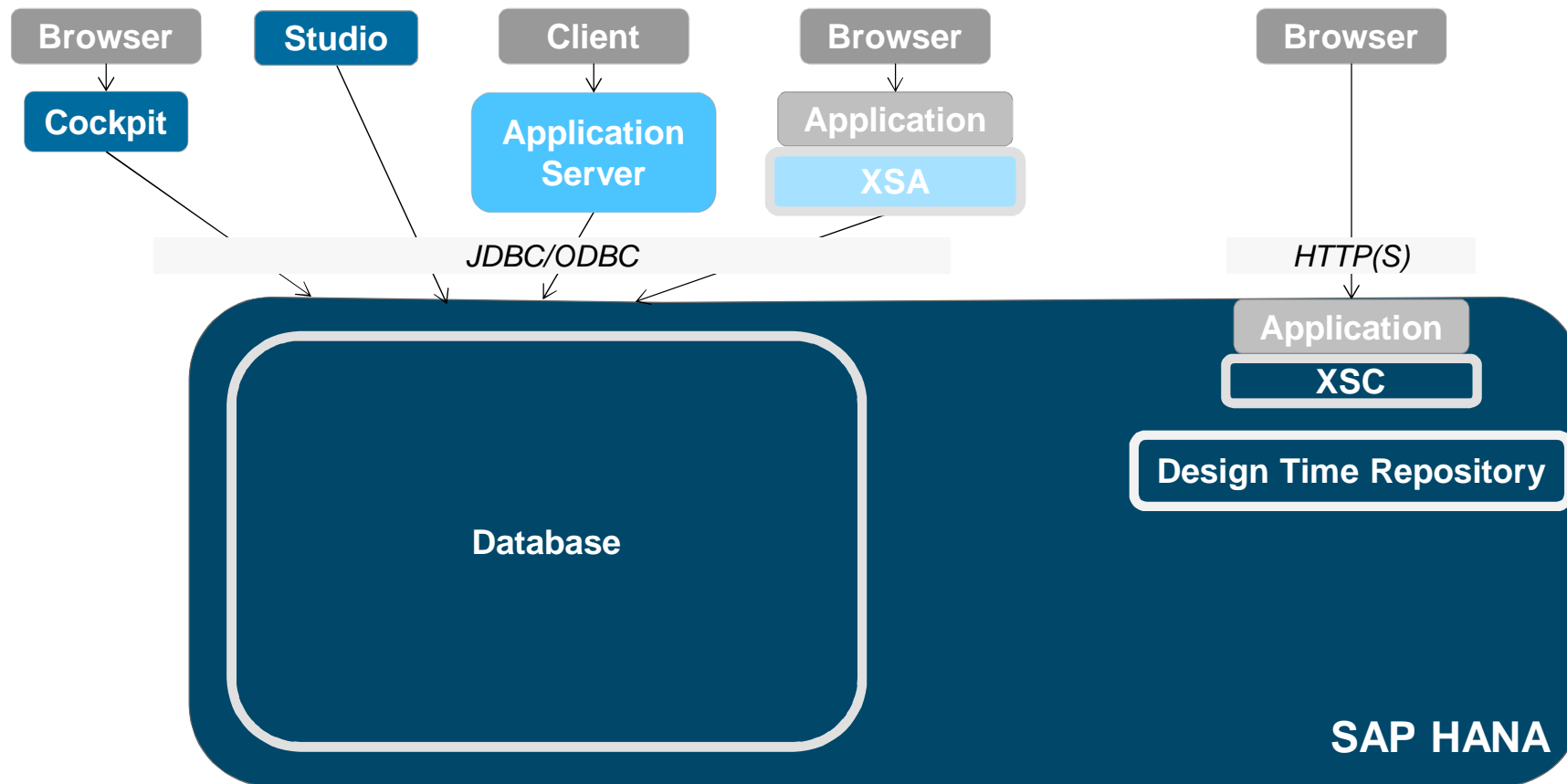
# Innovate with confidence on SAP HANA

## SAP HANA

- è **Runs securely in different environments**
- è **Helps you implement your specific security and compliance requirements**



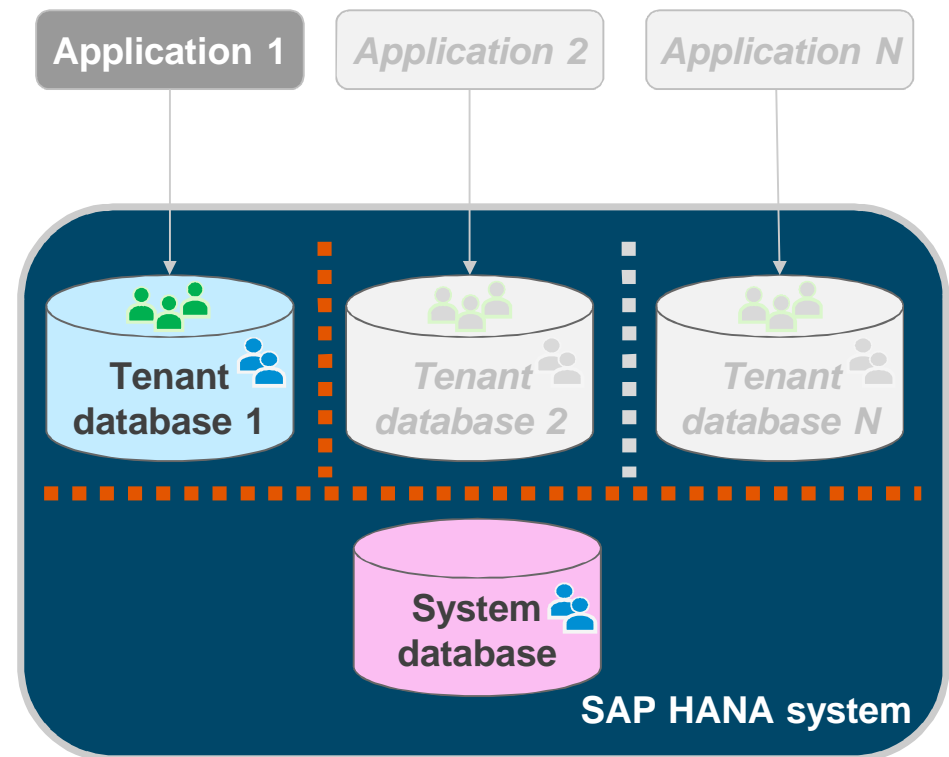
# SAP HANA's unified security architecture



# All systems run in multi-container database mode (as of SAP HANA 2.0 SPS01)

## Security benefits of multi-container database mode

- § Stronger protection of application data through isolation in dedicated tenant databases
  - Users, database catalog, repository, persistence, backups, traces and diagnosis files à per database
- § Segregation of duties
  - Separate administration for system and tenant databases
  - Separate networks for system administration and application access
  - Overall system administration from system database, but no access to tenant schemas from the system database
- § Hardening of tenant databases
  - Individual security configurations per tenant, e.g. TLS
  - Restrict exposed functionality and configuration options

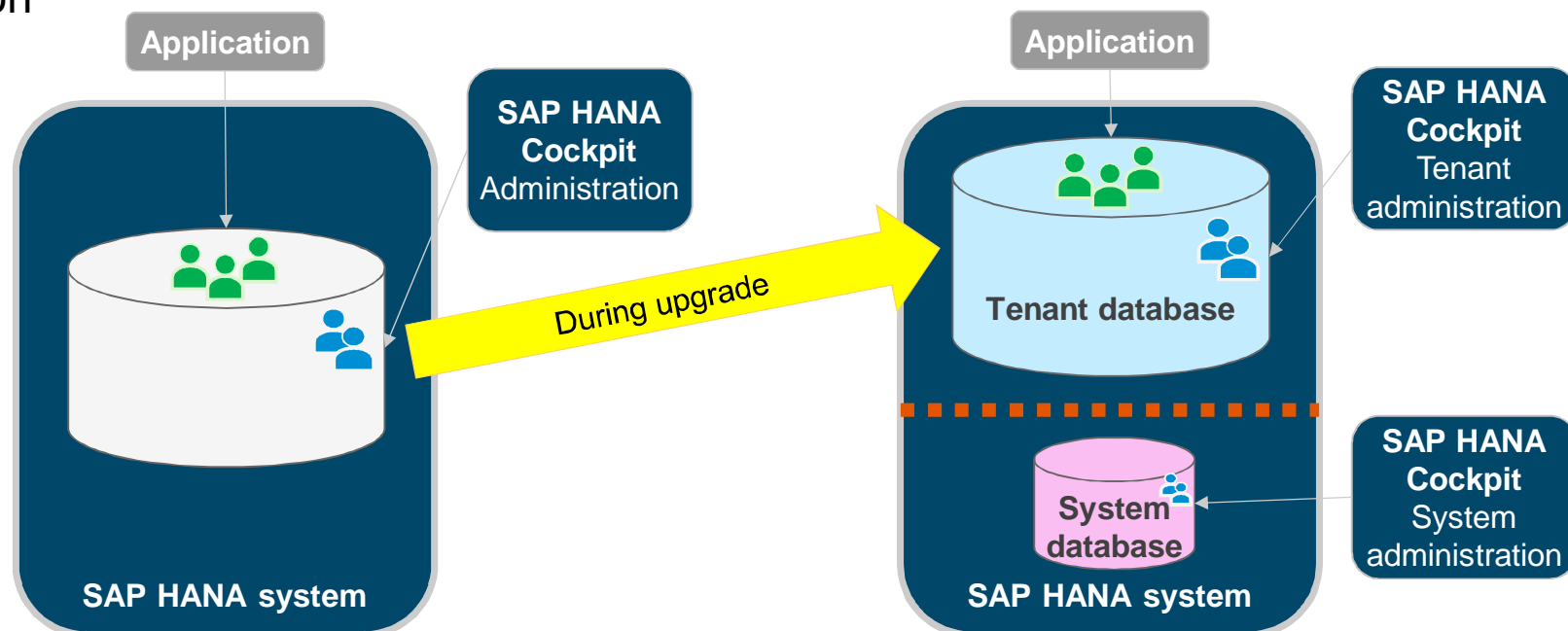


## What's new in SAP HANA 2.0 SPS01

All systems run in multi-container database mode – automatic conversion

**Automatic conversion of all single-container systems to multi-container database mode during upgrade to SAP HANA SPS01**

Converted system consists of 1 system database and 1 tenant database, inherits content and configuration



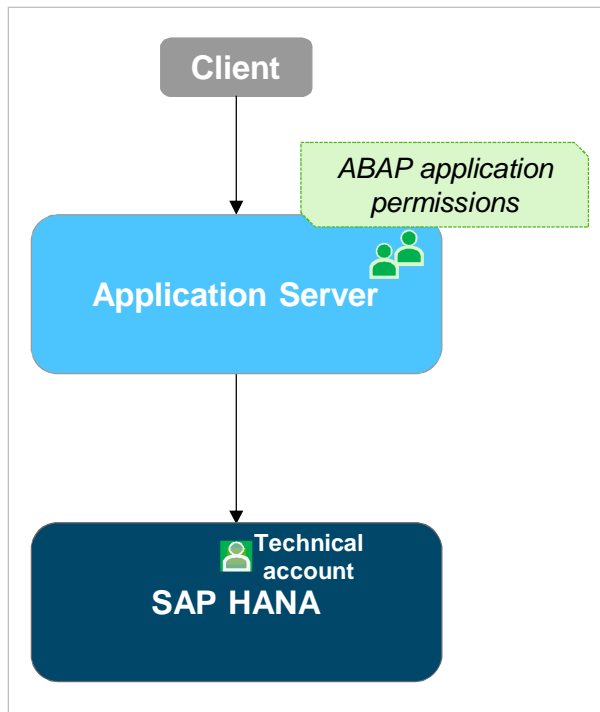
# Scenarios determine the security approach



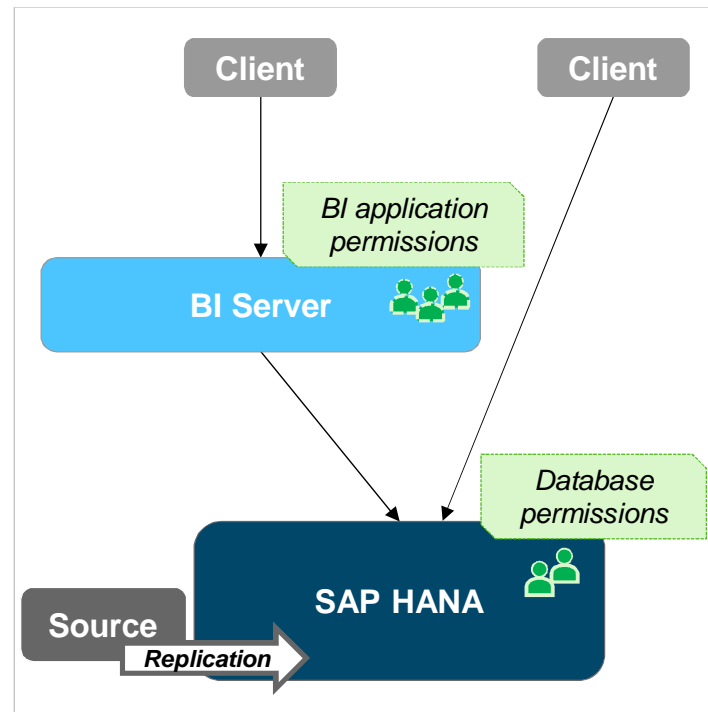


# SAP HANA scenarios – database, data mart, integrated reporting

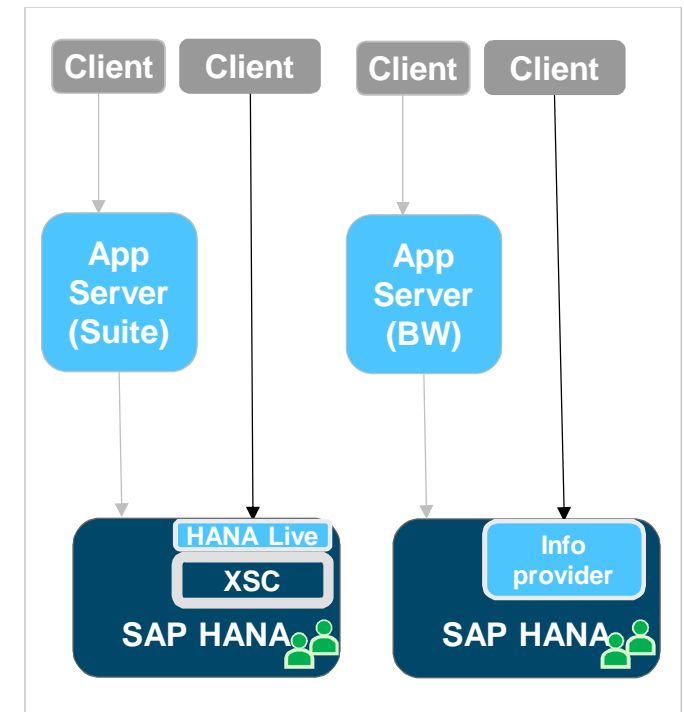
## Suite, BW, S4, BW4



## Data mart (3-tier or 2-tier)

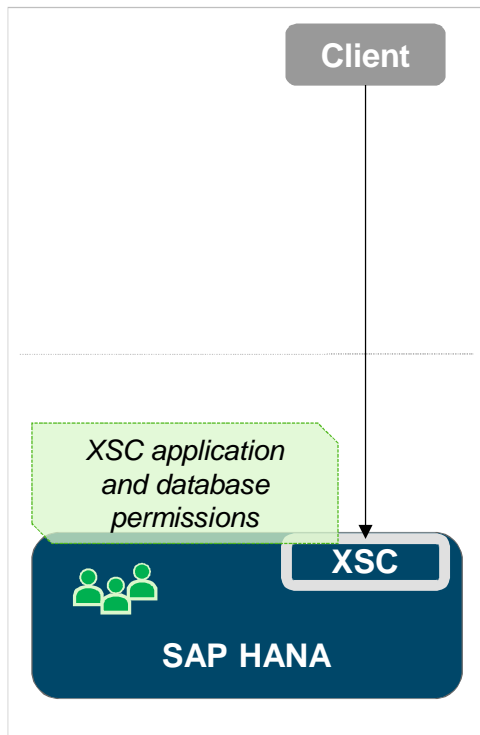


## Integrated reporting on Suite and BW data

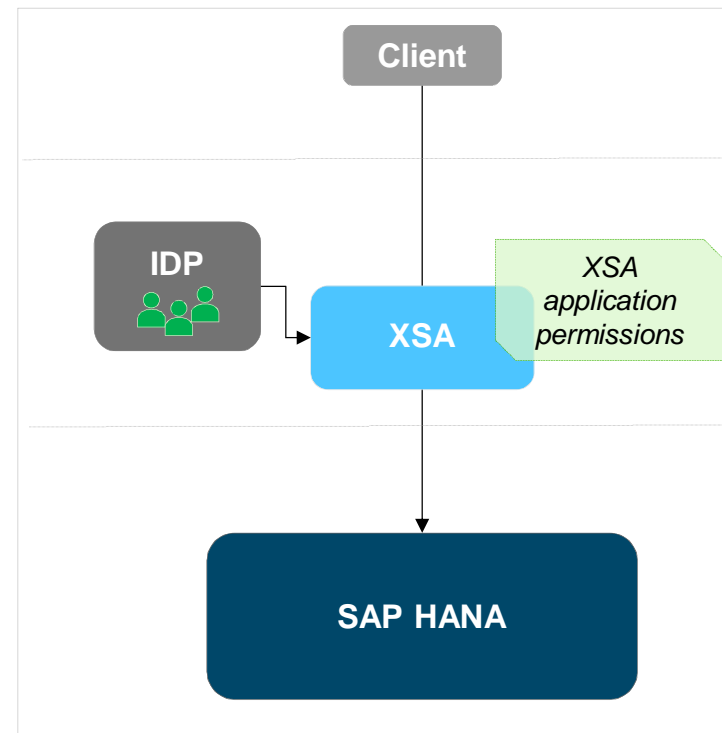


# SAP HANA scenarios – application development

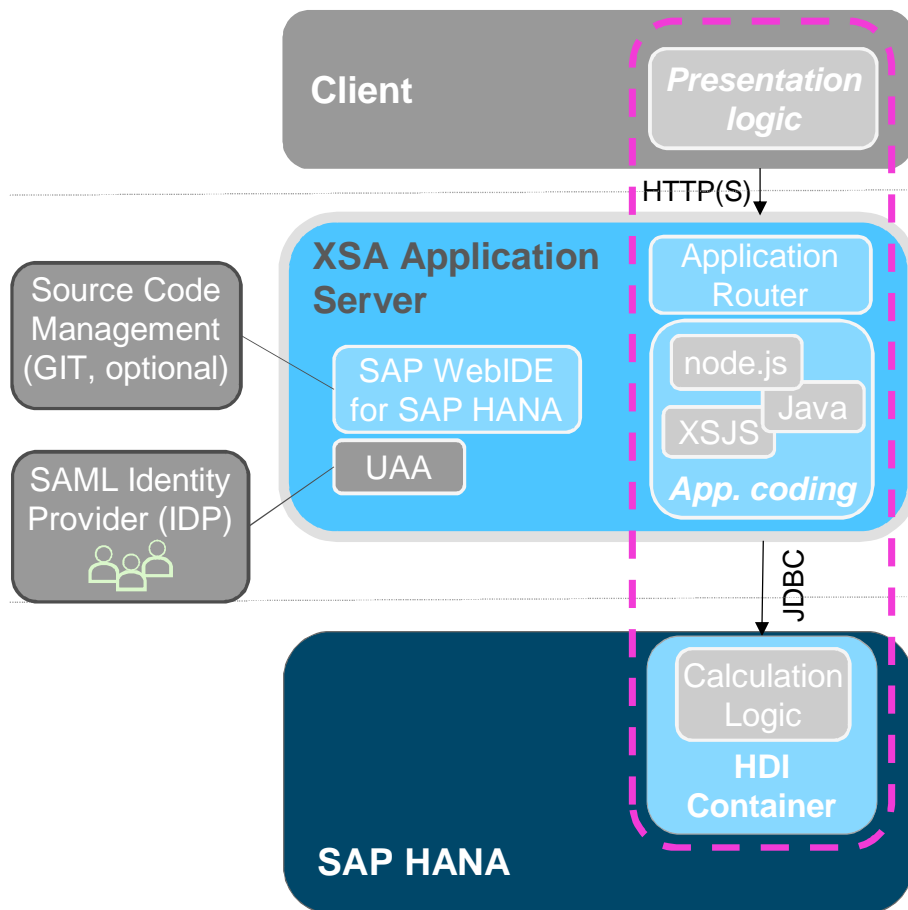
## XSC – integrated



## XSA – decoupled



# Applications built on SAP HANA XSA



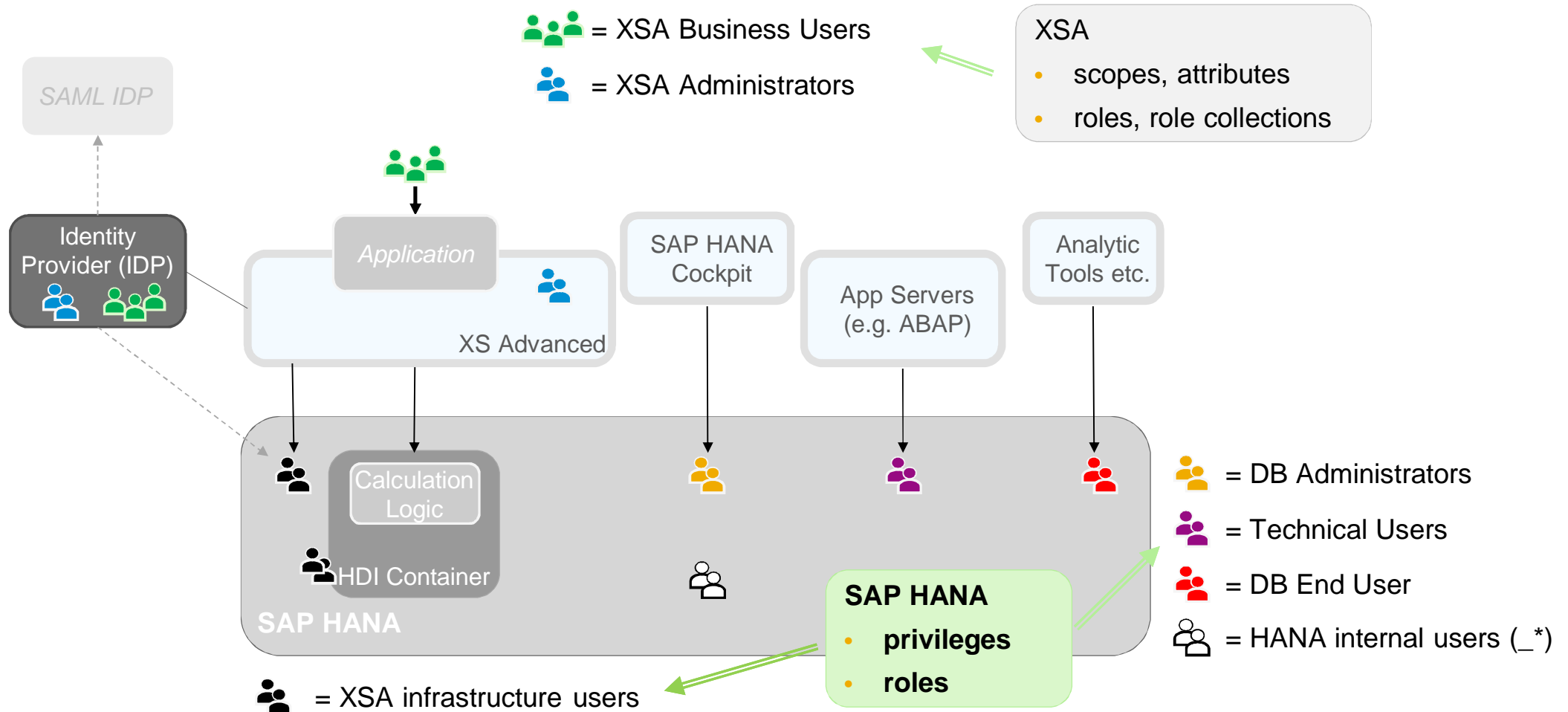
## Scalable, flexible application runtime with new security options

- § Decoupling of application layer and data layer
  - Separate deployment (e.g. network zones) and scaling of the XSA application layer
- § Isolation for applications
  - Data layer in SAP HANA: separate containers per application based on the SAP HANA Deployment Infrastructure (HDI)
  - XSA application layer: separate OS users per application (configurable)
- § XSA business users managed via identity provider
  - SAML2-compliant external identity provider, or
  - SAP HANA as native identity provider
  - Central user account and authentication server (UAA)
  - XSA business users authorized based on scopes and attributes
- § Source code management in GIT, new development tools

# Secure information access



## A closer look at users...



# User and identity management

## SAP HANA users

- § For logon a user in SAP HANA's user store is required
- § In some scenarios, end users don't need to log on to SAP HANA directly (e.g. S/4HANA, XSA)
- § Bootstrapping user SYSTEM created during installation. Recommendation: create dedicated administrators and lock user SYSTEM

## User administration and role assignment

- § SAP HANA Cockpit
- § Connectors for [SAP Identity Management](#), [SAP Access Control](#)
- § SQL interface for connecting custom solutions

The screenshot shows the 'Edit User' interface in the SAP HANA Cockpit for the user 'BUSINESSUSER'. The interface is divided into three tabs: 'GENERAL INFORMATION', 'AUTHENTICATION', and 'CUSTOM USER PROPERTIES'. The 'GENERAL INFORMATION' tab is active, showing fields for 'User Name' (BUSINESSUSER), 'Email' (john.miller@example.org), 'Valid From' (GMT+2), and 'Valid To' (GMT+2). Below these are three checkboxes: 'Creation of Objects in Own Schema' (Yes), 'PUBLIC Role' (Yes), and 'Disable ODBC/JDBC access' (No). The 'AUTHENTICATION' tab is also visible, showing the 'Authentication Mechanism' set to 'Password'. It includes fields for 'Password' and 'Confirm', and a checkbox for 'Force password change on next logon' (No). Other authentication mechanisms like 'Kerberos', 'SAP Logon Ticket', 'SAP Assertion Ticket', and 'SAML' are listed but not selected. The bottom of the interface has 'Save' and 'Cancel' buttons.

# User types

## Standard users


- § Standard users can create objects in their own schema.
- § They have read access to system views via the PUBLIC role, which is granted to every standard user.

## Restricted users

- § Restricted users initially have no privileges. This user type is intended for users who access SAP HANA through client applications and do not need full SQL access via an SQL console.
- § Compared to standard database users, restricted users
  - Cannot create objects in their own schema
  - Cannot view any data (e.g. system views) in the database as they do not have the PUBLIC role
    - To enable a restricted user to use an application, grant the required application-specific roles.
    - Initially restricted users can only connect to the database using HTTP/HTTPS. For restricted users to connect via ODBC or JDBC, enable ODBC/JDBC access explicitly.

**Restricted users can be converted to standard users, and vice versa**

# Restricted user handling in SAP HANA cockpit

 SAP HANA Cockpit | H21@H21 (PRODUCTION)

Edit User 'RESTRICTED1'

GENERAL INFORMATION

AUTHENTICATION

CUSTOM USER PROPERTIES

User Name:

RESTRICTED1

Email:

Valid From:

3/7/17, 1:39 PM

GMT+1

Valid To:

M/d/yy, h:mm a

GMT+1

Creation of Objects in Own Schema:

☐ Yes ☒ No

PUBLIC Role:

☐ Yes ☒ No

Disable ODBC/JDBC access:

☒ Yes ☐ No



# Comprehensive role and privilege framework

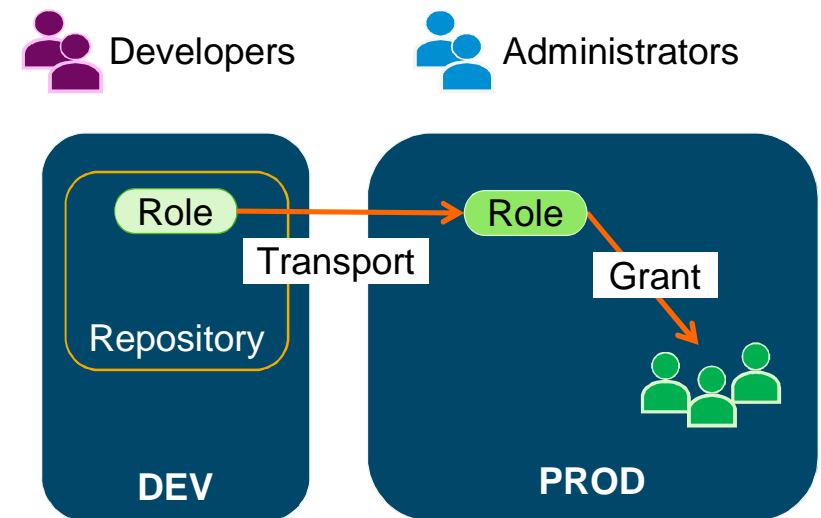
**SAP HANA's authorization framework provides highly granular access control**

**Roles** are used to bundle and structure privileges for dedicated groups of users

§ Role transport available for DEV/QA/PROD system landscapes (for repository roles)

§ LDAP integration

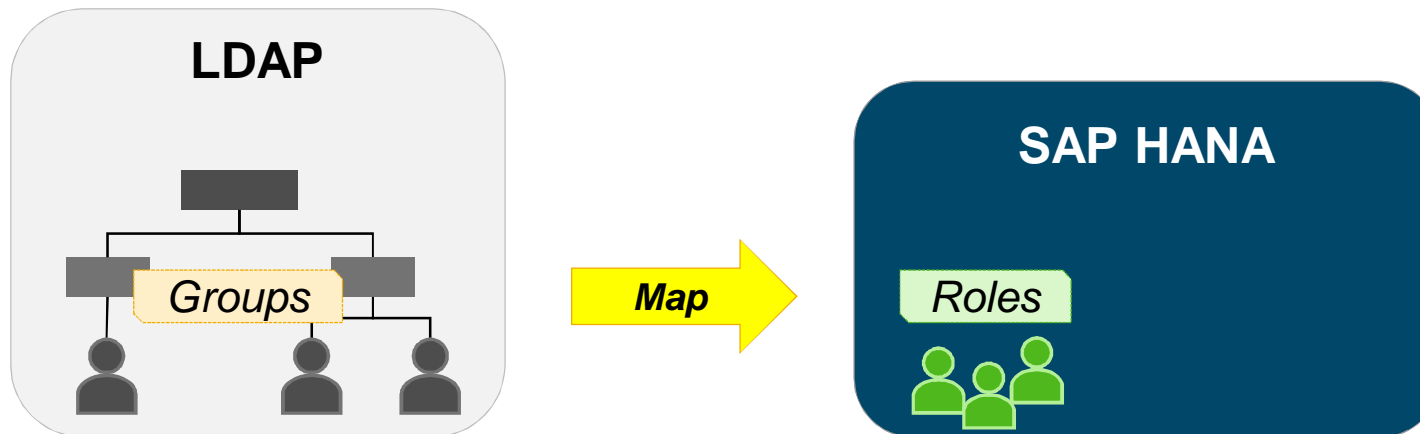
§ [SAP Access Control](#) support



# LDAP group authorization

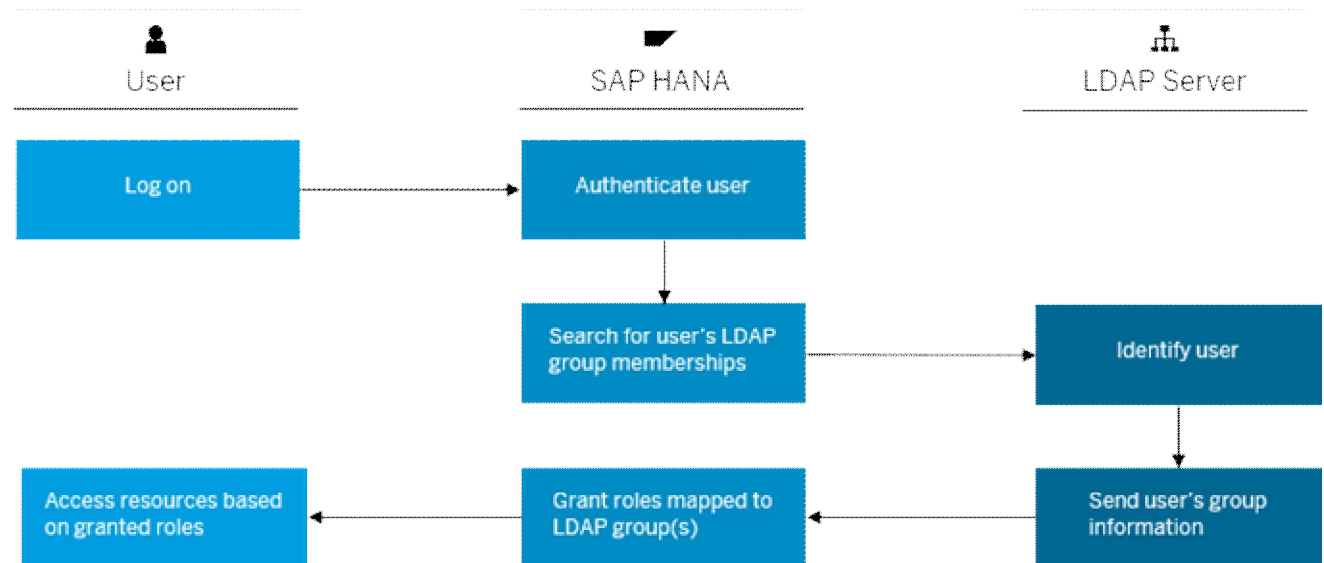
## LDAP groups can now be used for automatic role assignment in SAP HANA

§ Using an LDAP server as a central repository significantly reduces complexity for maintaining authorizations in large system landscapes.



# LDAP group authorization – how does it work?

1. LDAP-enabled user logs on
2. SAP HANA queries the LDAP directory for group memberships
  - Logon to SAP HANA succeeds if the user's LDAP groups map to at least one SAP HANA role.
  - Logon to SAP HANA fails if the user is not member of any LDAP groups, or the groups are not mapped to any SAP HANA roles
3. SAP HANA grants the user roles according to the defined mapping
  - LDAP group memberships are cached (default 4 hours). However you can configure the caching duration, e.g. force the LDAP group membership to be re-evaluated upon each user logon.

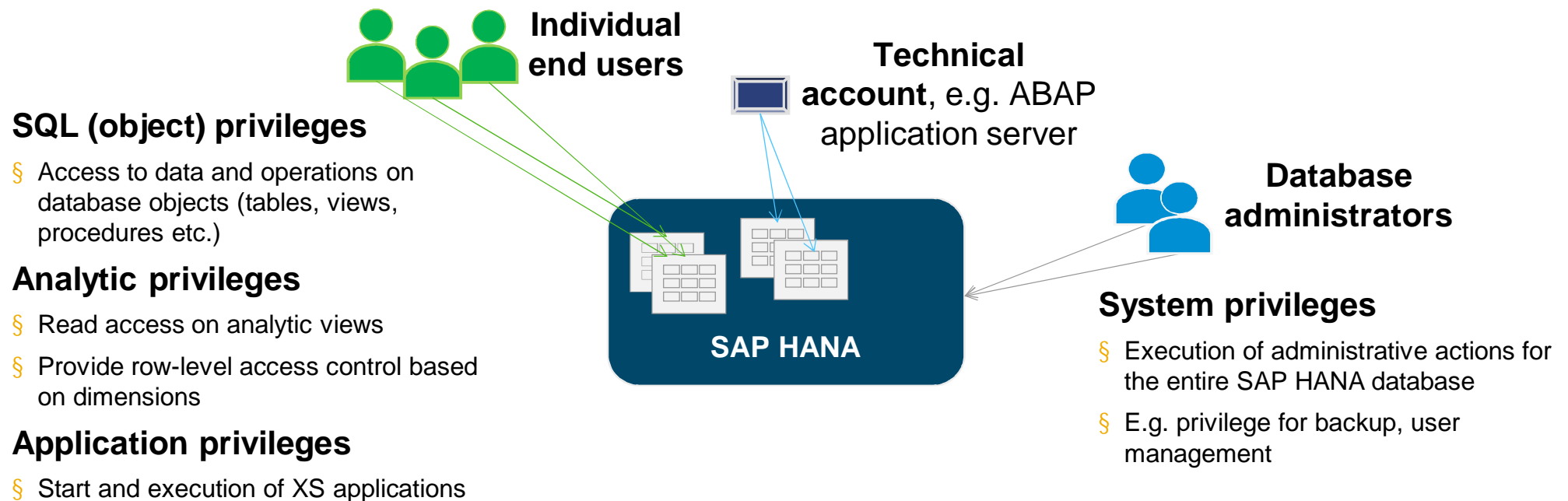


**Note:** LDAP group authorization needs to be explicitly enabled for users.

# SAP HANA – database access privileges

**Privileges define what users can see and do: no privilege – no access!**

§ Based on standard SQL object privileges, with SAP HANA-specific extensions for business applications



# Authorization – row-level access control using analytic privileges

## Goal


Protect row-level data based on column attributes.

Account	Sales Region	Revenue 2017
1145	EMEA	223000
1267	APJ	12500
2105	US	455690
3120	APJ	226800
1896	EMEA	159000

## Example

§ **Account manager Miller** is responsible for the **US** sales region and will see all rows containing US data, but not rows containing data from other sales regions.

§ **Account manager Stephens** is responsible for the **EMEA** sales region and will see only rows containing EMEA data.

  
Account  
manager  
Miller

SALES APPLICATION		
Account	Sales Region	Revenue 2017
2105	US	455690

  
Account  
manager  
Stephens

SALES APPLICATION		
Account	Sales Region	Revenue 2017
1145	EMEA	223000
1896	EMEA	159000

# Dynamic data masking

## Goal

Protect sensitive data with the option to display partial information or completely masked information.

## Example

§ **A call center agent** uses the call center application to work on customer requests. The agent asks for the last 4 digits of a customer's credit card number in order to proceed with questions about recent credit card transactions. The call center agent does not need the full credit card number.

§ **If customer Ann** logs on to the self service portal of the bank, he/she will of course be able to see the full credit card number.

Name	Credit Card Number	Actions
Meyer, Joe	1234-5678-9012-3456	<a href="#">Transactions</a>
Miller, Ann	9876-5432-1098-7654	<a href="#">Transactions</a>
Newman, Ron	5678-9012-3456-1234	<a href="#">Transactions</a>
Powers, Judy	6789-0123-4567-2345	<a href="#">Transactions</a>
Richmond, Paul	2109-8765-4321-6543	<a href="#">Transactions</a>



CALL CENTER APPLICATION		
Name	Credit Card Number	Actions
Meyer, Joe	xxxx-xxxx-xxxx-3456	<a href="#">Transactions</a>
Miller, Ann	xxxx-xxxx-xxxx-7654	<a href="#">Transactions</a>



CUSTOMER SELF SERVICE APPLICATION		
Name	Credit Card Number	Actions
Miller, Ann	9876-5432-1098-7654	<a href="#">Transactions</a>

## Dynamic data masking – which users see what?

- è **Data masking is an additional layer of access control applied to views**
- è **Fully integrated into SAP HANA's authorization framework**
  - SAP HANA can still execute calculations as usual
  - Mask expressions defined on columns of a view; can use constants, built-in and user-defined function

### New object privilege UNMASKED

		SELECT privilege	
		Not granted	Granted
UNMASKED privilege	Not granted	Not authorized	####-####-####-7654
	Granted	Not authorized	9876-5432-1098-7654

# Demo: Dynamic Data Masking



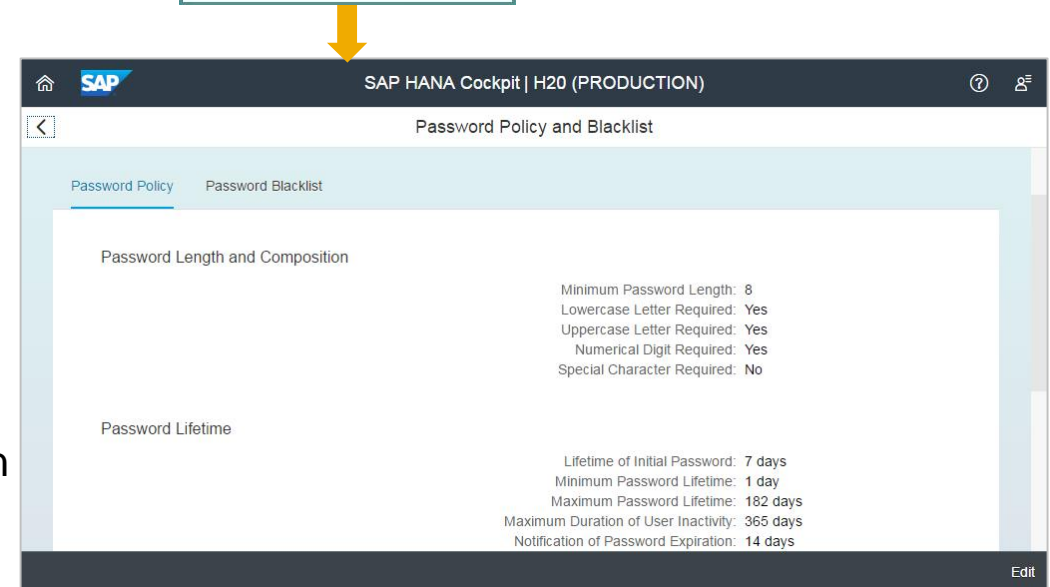
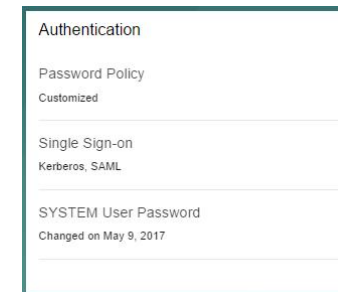
# Authentication and single sign-on

## Access to SAP HANA data, functions and applications requires authentication

- § Authentication options configurable per user
  - Password login
    - Note that there are no default passwords
  - Single sign-on: Kerberos/SPNEGO, SAML, JWT, SAP logon and assertion tickets, X.509 (XSC)

## Default password policy that applies to all users who log on with user name/password

- § The password policy e.g. specifies the strength of passwords and the password change schedule
- § You can customize the password policy and maintain a password blacklist



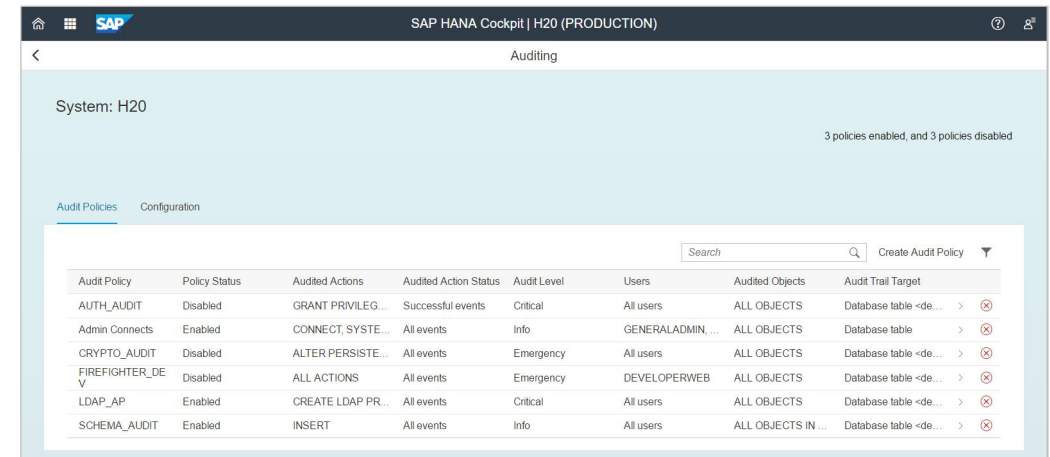
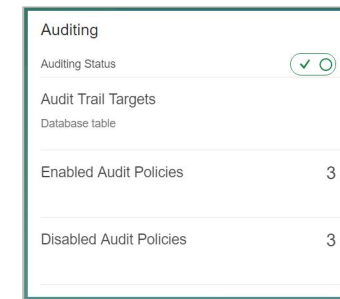
# Audit logging

## Audit logging records critical system events

- § User management: e.g. user/role changes
- § System access/configuration: e.g. failed logons
- § Data access: e.g. read or write access to tables and views, procedure execution
- § Firefighter (audit all): e.g. for support access

## Audit policies include the events to be recorded

- § If audit logging is enabled, some critical events are always logged, e.g. disabling of audit logging
- § Audit events are logged in the audit trail
  - Linux syslog or secure database table



# Audit logging – examples for audit policies

## Policy 1 (user changes)

Audited Actions:

- CREATE USER
- ALTER USER
- DROP USER

## Policy 3 (access to data)

Audited Actions:

- SELECT
- INSERT

Audited Objects:

- "SCHEMA" . "TABLE"

## Mandatory Policy

Audited Actions:

- DROP AUDIT POLICY
- ALTER SYSTEM CLEAR AUDIT LOG
- ...

## Policy 2 (table management)

Audited Actions:

- CREATE TABLE
- ALTER TABLE
- ...

## Policy 4 (firefighter)



Audited Actions:

- ALL

Audited Users:

- DBADMIN

# Audit logging – supported audit trail targets

## syslog

```
2017-06-30
13:04:54;indexserver;myhanablade23.cu
stomer.corp;HAN;01;30103;10.29.14.177
;lu306309;6776;58060;Alter User
Policy;INFO;ALTER
USER;SYSTEM;ADAMS;SUCCESSFUL;
;alter user ADAMS
VAXXXXXXXXXXXXXX;434597;

2017-06-30 02:04:54 -----
-----
```

- § Secure
- § Flexible, e.g. direct audit trail to remote server
- § Can be integrated into landscape
- § Must be configured correctly

## "PUBLIC"."AUDIT\_LOG"

TIME STAMP	HOST	USER	POLICY	LEVEL	OBJECT	STATE MENT
10-Jun-2017 15:44:53	myhanablade23.cu stomer.c orp	DBAADMIN	Mandator yAuditPo licy	CRITICAL	-----	CREATE AUDIT POLICY
10-Jun-2017 10:42:23 .0	-----	-----	-----	-----	-----	-----

- § Secure
- § Requires specific system privileges
- § Data can be accessed and analyzed directly in SAP HANA
- § No further configuration required

# Data protection and privacy (DPP)

**SAP HANA provides the technical enablement and infrastructure to allow you to run applications that conform to DPP requirements**

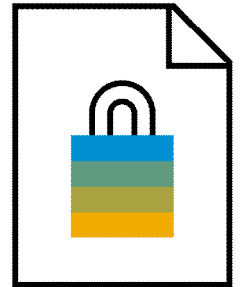
DPP requirements:

- § Legal (new European General Data Protection Regulation/GDPR)
- § Industry standards
- § Companies' strategic business decisions.

è Dependent on business semantics and context

è SAP HANA provides all the features that applications require to flexibly implement DPP requirements within the context of the business use case

- § Access control, access logging, communication security, availability control, separation by purpose, deletion of personal data



# Data protection and privacy (DPP)

DPP Aspect	SAP HANA Features
<b>Access control</b>	<ul style="list-style-type: none"><li>• Authentication</li><li>• Authorization</li><li>• Data masking</li><li>• Data encryption (for example, data volume encryption, redo log encryption, backup encryption)</li></ul>
<b>Access logging</b>	<ul style="list-style-type: none"><li>• Audit logging</li></ul>
<b>Communication security</b>	<ul style="list-style-type: none"><li>• Support for encrypted communication on all internal and external channels</li></ul>
<b>Availability control</b>	<ul style="list-style-type: none"><li>• Backup and recovery</li><li>• Storage replication and system replication</li><li>• Service auto-restart and host auto-failover</li></ul>
<b>Separation by purpose</b>	<ul style="list-style-type: none"><li>• Authorization</li><li>• Schemas</li><li>• Multi-container database mode/tenant isolation</li></ul>
<b>Deletion of personal data</b>	<ul style="list-style-type: none"><li>• Data deletion</li></ul>

# Secure configuration and operations





# Overview: secure system setup

## SAP HANA is designed to run securely in different environments

Incorrectly configured security settings are one of the most common causes of security problems!

è SAP offers **information** and **tools** to help you to run SAP HANA securely

- [SAP HANA security guide](#) (incl. chapter on data protection)
- [SAP HANA security checklists](#)

The screenshot shows a document titled "SAP HANA Security Checklists and Recommendations". It includes a section "About this Document" with bullet points: "The checklists and recommendations contained in this document are not exhaustive... your specific implementation scenario and technical environment, some of the... or be different.", "Do not use the checks contained in this document as instructions on how to... particular check result indicates an insecure setting... refer to the indicated docu... instructions there to change the configuration setting.", and "This document does not replace the SAP HANA Security Guide, the central docu... to the secure operation and configuration of SAP HANA." Below this is a "General Recommendations" section with "Checklist for Secure Handover" and a note: "If you received your SAP HANA system pre-installed from a hardware or hosting partner, we strongly recommend you do immediately after handover."

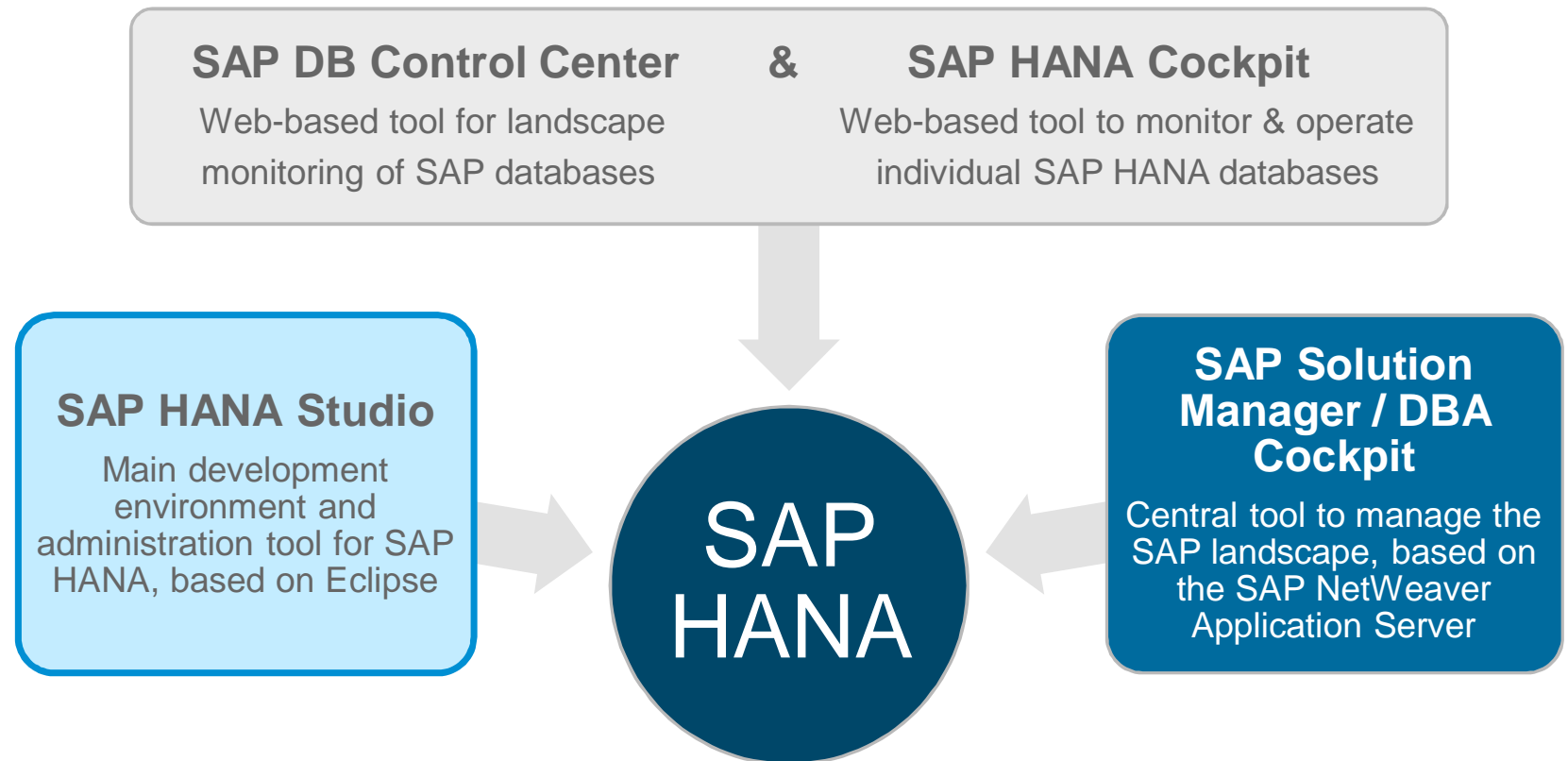
The screenshot shows the "SAP HANA Security Guide" document. It features a "Table of Contents" on the left with links to "SAP HANA Security Guide", "Security Information Map", "SAP HANA Security Patches", "SAP HANA Overview", "SAP HANA Network and Communication Security", "SAP HANA User Management", "SAP HANA Authentication and Single Sign-On", "SAP HANA Authorization", "Data Storage Security in SAP HANA", "Data Protection in SAP HANA", "Auditing Activity in SAP HANA Systems", and "Certificate Management in SAP HANA". The main content area is titled "SAP HANA Security Guide" and includes a "Note" stating: "This guide does not cover security-relevant information for SAP HANA options and capabilities, such as SAP HANA dynamic tiering and SAP HANA smart data streaming. For more information about the security of options and capabilities, see the documentation of the relevant SAP HANA option on SAP Help Portal. Be aware that you need additional licenses for SAP HANA options and capabilities. For more information, see Important Disclaimer for Features in SAP HANA Platform, Options and Capabilities." Below the note is a section "Why is Security Necessary?" with text: "Protecting corporate information is one of the most important topics for you as an SAP HANA customer. You need to meet ever increasing cyber-security challenges, keep your systems secure, and stay on top of the compliance and regulatory requirements of today's digital world. SAP HANA allows you to securely run and operate SAP HANA in a variety of environments and to implement your specific compliance, security, and regulatory requirements." The bottom section is titled "Important Critical Configurations".



# Administration Tools Overview: SAP HANA 1.0 SPS09 – SPS12

## § SAP HANA 1.0 SPS09 – SPS12:

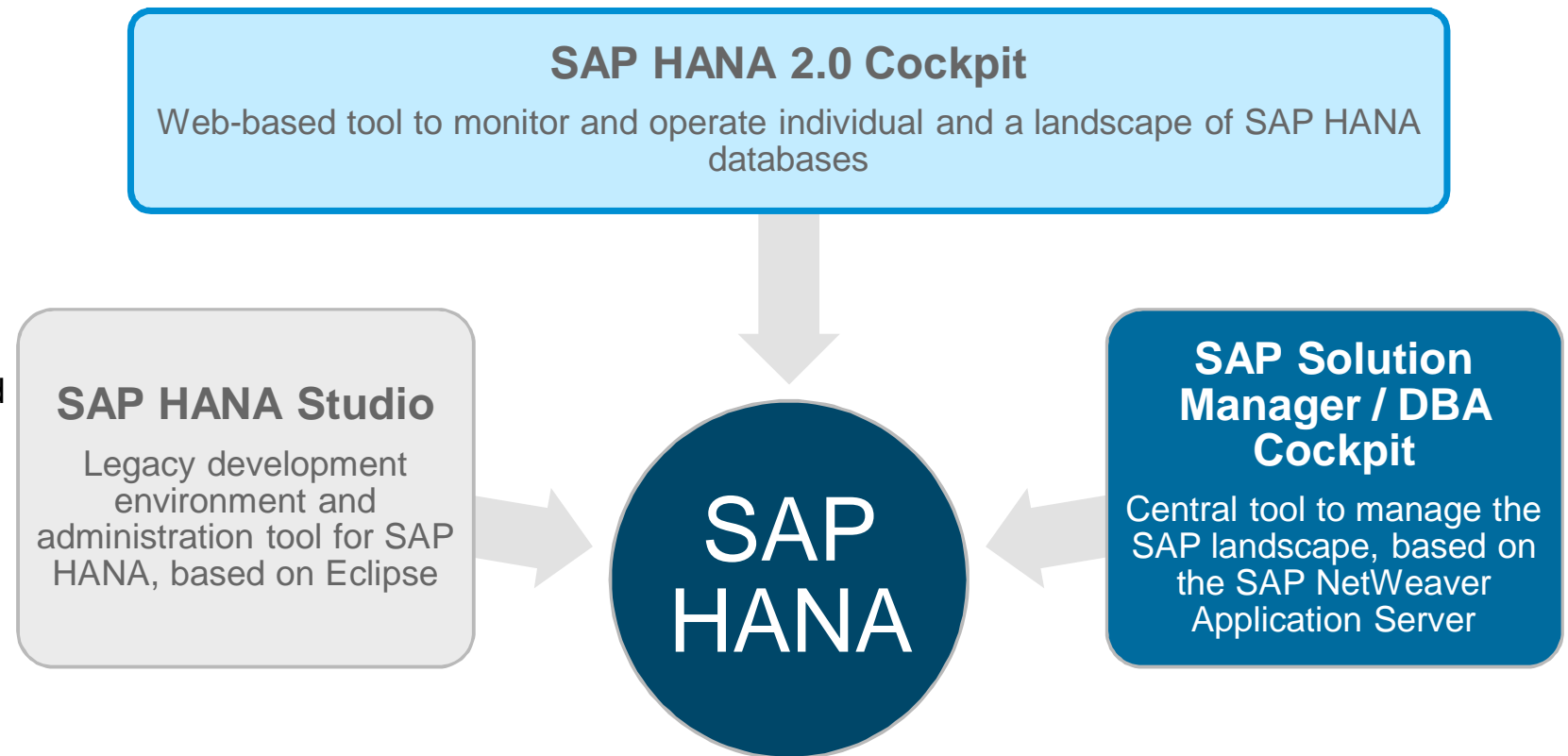
- Eclipse-based SAP HANA studio is the main development environment and the main administration tool for SAP HANA databases.
- Web-based SAP DB control center and SAP HANA cockpit are introduced to monitor SAP HANA.
- SAP HANA is fully integrated into SAP Solution Manager.



# Administration Tools Overview: SAP HANA 2.0

§ In SAP HANA 2.0:

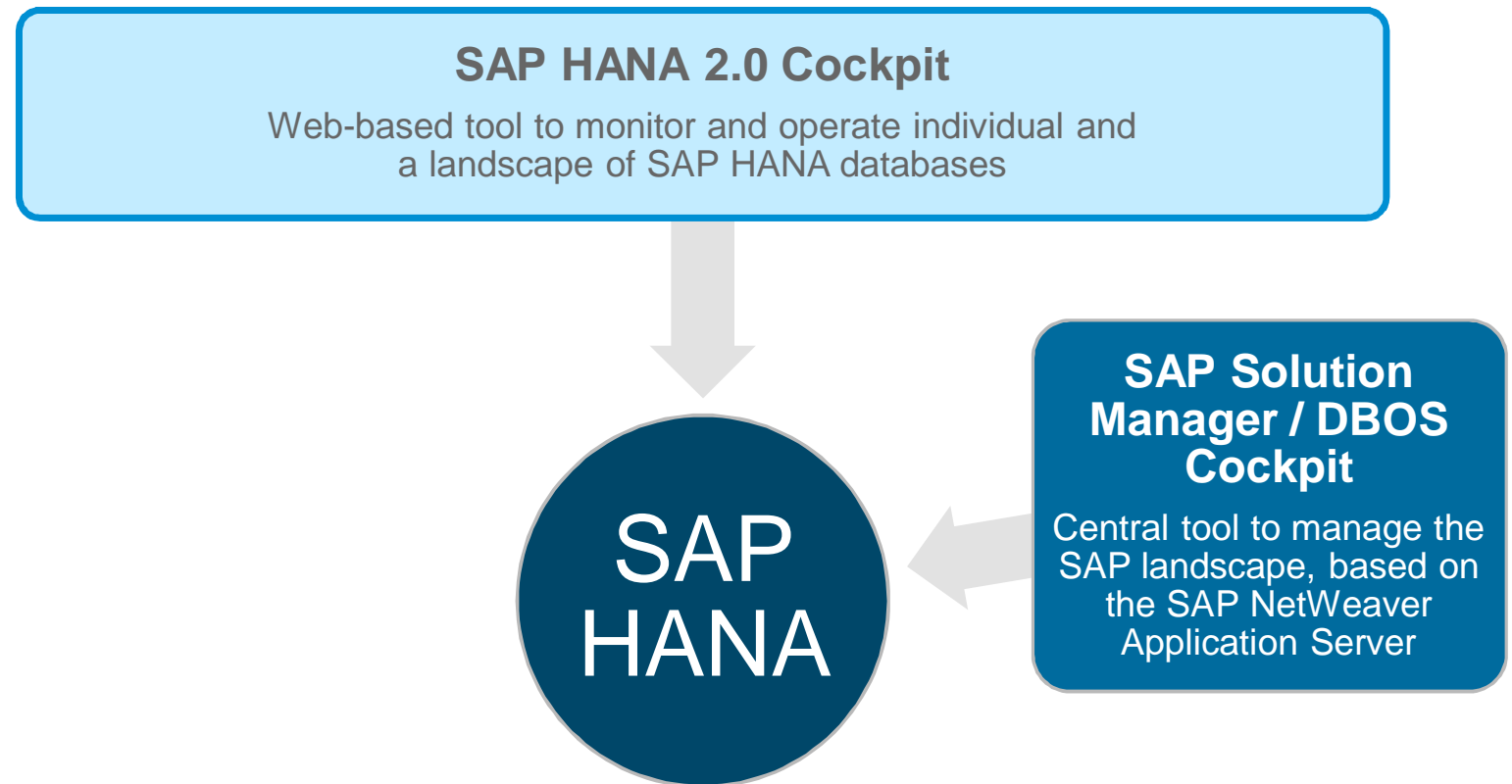
- SAP HANA studio is still supported, but no new features are being added.
- SAP DB control center and SAP HANA cockpit functionality is combined into a new free-standing SAP HANA 2.0 cockpit.
- Cockpit is backwards-compatible to SAP HANA 1.0 SPS12
- SAP HANA is fully integrated into SAP Solution Manager.



# Administration Tools Overview: Future

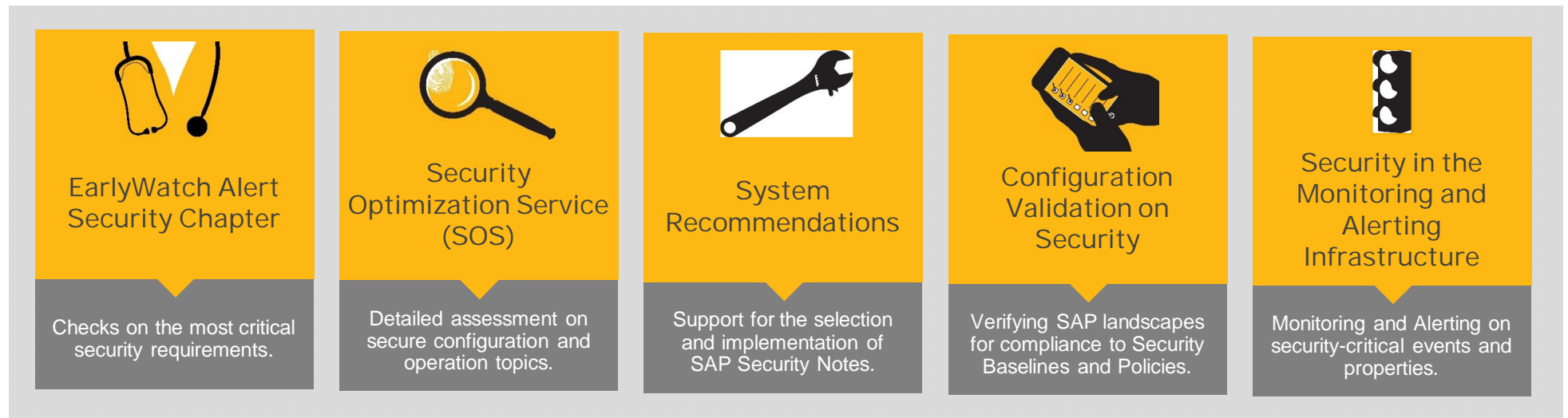
## § Future plans:

- Following SAP's cloud strategy, SAP HANA offers web-based tools for monitoring and administration.
- SAP HANA cockpit follows an alert-driven guided-procedure approach. A DBA will be enabled to drill-down to the root cause of an issue.
- SAP HANA cockpit will replace the administration perspective of HANA studio in the long term.



This is the current state of planning and may be changed by SAP at any time.

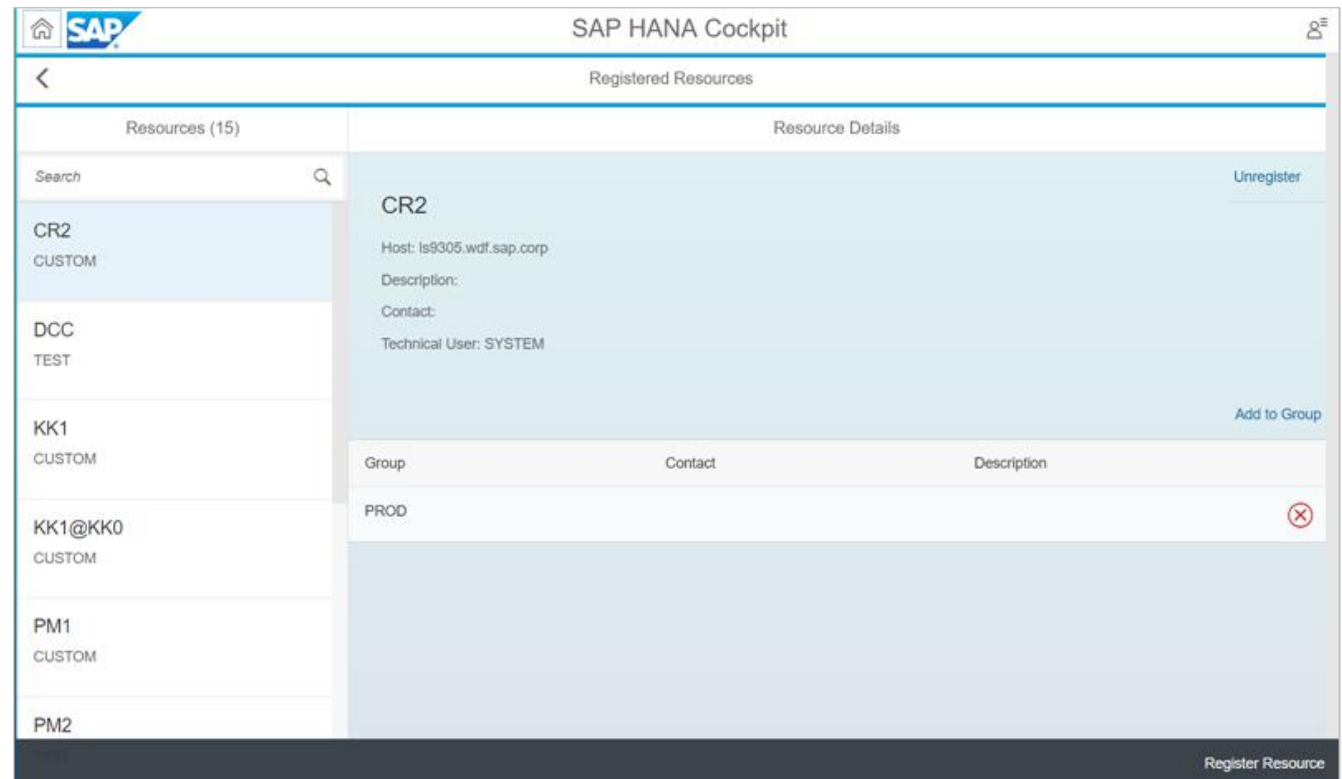
## Overview: integration with SAP's security tools and services



# Cockpit Manager

## Cockpit Manager manages resources (SAP HANA systems)

- § Register resources
- § Organize resources in groups
- § Manage Cockpit users
- § Access from Cockpit landscape page



# Cockpit Landscape Overview and Group Pages

## Provides views and actions across many resources (HANA systems)

- § Resource directory
- § Global view of alerts
- § Groups of resources
- § Aggregate health monitor
- § Compare configurations
- § Recently accesses resources
- § Access Cockpit Manager
- § Launch Database Explorer

The screenshot displays the SAP HANA Cockpit interface. At the top, a navigation bar includes links for 'EST', 'MDC Tenants', 'PROD', 'SPS12', and 'Single Container', each with a red alert count (5, 1, 10, 7, 4 respectively). The main section is titled 'My Resources' and shows 'All resources available to me'. A large number '13' indicates the total number of resources. Below this, a 'Top Resources with Alerts' section lists five resources with their respective alert counts: TSS (5), PM2 (4), SXE (3), PM1 (2), and DCC (1). Each resource entry includes its name, ID, and environment (e.g., CUSTOM, TEST). To the right, a 'Recently Accessed' table lists resources accessed recently, including CR2, TN1@TS2, W40, TSS, and SYSTEMDB@MDC, along with their host names and usage types. The bottom of the interface features three main sections: 'Administration' (with links for monitoring health, viewing resources, comparing configurations, and managing cockpit), 'Database Explorer' (with links for browsing objects and executing SQL), and 'Help' (with a link for administration help).

Name	Host Name	Usage
CR2	ls9305.wdf.sap.corp	CUSTOM
TN1@TS2	mo-359527ea7.mo.sap....	CUSTOM
W40	mo-fb4bd2e2a.mo.sap.c...	TEST
TSS	mo-359527ea7.mo.sap....	CUSTOM
SYSTEMDB@MDC	mo-303b8718d.mo.sap....	CUSTOM



# Database Explorer

## Connect to multiple HANA systems or HDI Containers

### § Catalog browser

- Tables, procedures, sequences, views,...
- Search across multiple systems
- Import catalog objects

### § SQL Console

- Syntax highlighting and autocomplete
- View, sort, and export result sets

### § Access trace files

The screenshot displays the SAP HANA Database Explorer interface. On the left, a catalog browser shows a tree structure of database objects under the 'TSS' connection. The 'Tables' folder is selected, and a search list below it shows tables like 'MACHINE\_READINGS', 'STOCK', 'VIBRATION', 'WEATHER\_HOURLY', 'WEATHER\_NULLS\_HOURLY', and 'WEATHER\_ORIG'. The main pane shows a table named 'WEATHER\_HOURLY' with columns 'SENSOR', 'TIMER', and 'TMP'. The table contains 22 rows of data. On the right, a search panel is visible with the text '0 search results (Specify at least two characters)' and a 'Select/Deselect All' checkbox. Below the search panel, there are checkboxes for 'Table', 'View', 'Proce', 'Functi', 'Sequi', 'Trigge', 'Index', 'Synon', 'Comm', 'Scher', and 'Defini'.

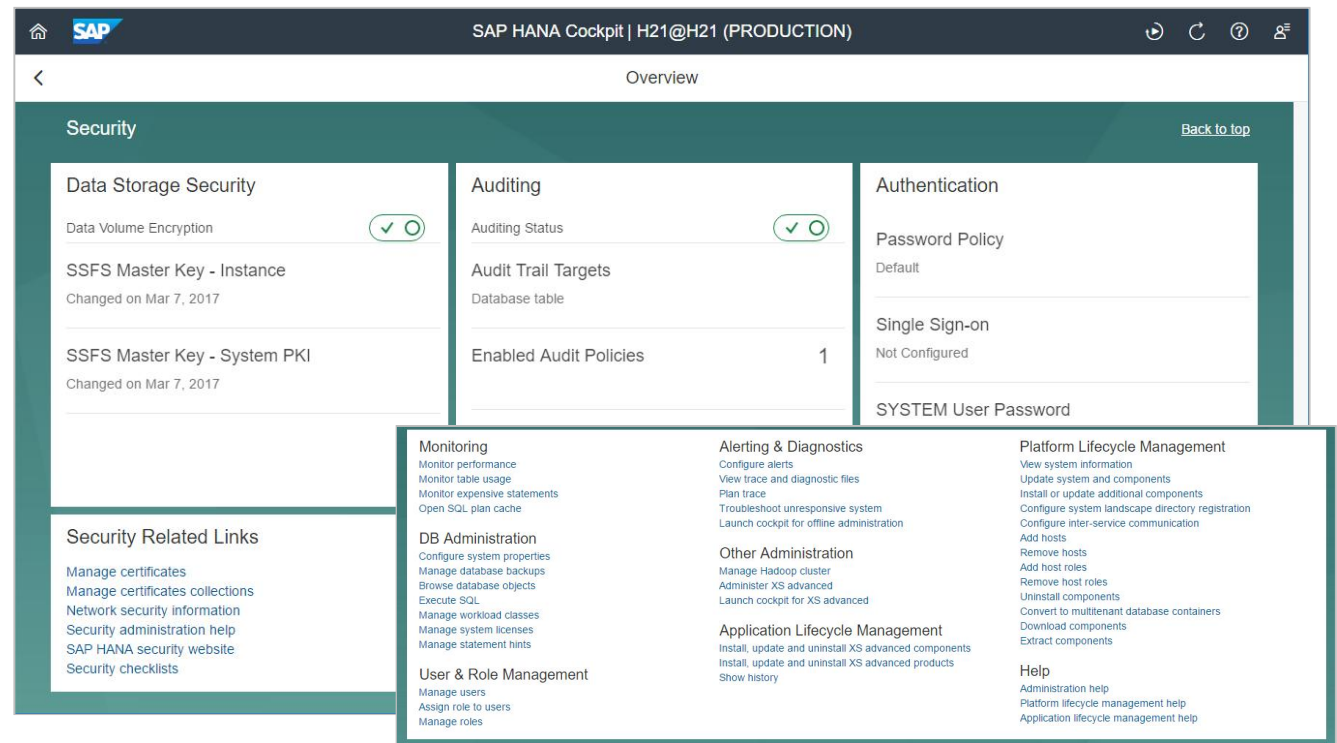
	SENSOR	TIMER	TMP
1	OTM	2014-07-01T01:00:00.00	71.01
2	OTM	2014-07-01T02:00:00.00	68.35
3	OTM	2014-07-01T05:00:00.00	68.73
4	OTM	2014-07-06T00:00:00.00	67.41
5	OTM	2014-07-06T01:00:00.00	67.61
6	OTM	2014-07-06T02:00:00.00	69
7	OTM	2014-07-10T06:00:00.00	69.21
8	OTM	2014-07-14T09:00:00.00	67.86
9	OTM	2014-07-14T10:00:00.00	67.35
10	OTM	2014-07-14T13:00:00.00	67.1
11	OTM	2014-07-14T16:00:00.00	66.95
12	OTM	2014-07-23T11:00:00.00	69.08
13	OTM	2014-07-23T12:00:00.00	68.03
14	OTM	2014-07-23T13:00:00.00	66.91
15	OTM	2014-07-26T13:00:00.00	68.06
16	OTM	2014-07-26T14:00:00.00	67.16
17	OTM	2014-07-26T15:00:00.00	67.05
18	OTM	2014-07-26T18:00:00.00	67.28
19	OTM	2014-07-26T19:00:00.00	68.55
20	OTM	2014-08-04T12:00:00.00	68.08
21	OTM	2014-08-04T13:00:00.00	67.48
22	OTM	2014-08-04T14:00:00.00	67.83



# Security management in SAP HANA cockpit

**SAP HANA cockpit lets you monitor the security status of your system and provides easy access to the security configuration.**

- § Data storage security/encryption
- § Auditing
- § Authentication
- § User/role management
- § Certificate management
- § Network security information
- § Links to relevant security resources such as the security guide and check lists



# Security apps in the SAP HANA cockpit

The image displays three overlapping screenshots of the SAP HANA Cockpit interface, specifically the 'H20 (PRODUCTION)' environment. The top-left screenshot shows the 'Data Volume Encryption' page, which includes a table titled 'Encryption Status of Services'. The top-right screenshot shows the 'Password Policy and Blacklist' page, with tabs for 'Password Policy' and 'Password Blacklist'. The bottom-left screenshot shows the 'Auditing' page, with tabs for 'Audit Policies' and 'Configuration'. The 'Audit Policies' tab is active, displaying a table of audit policies.

Host	Service	Port	Root Key Change Pending	Current Key Version	Status
mo-97cb5c502	indexserver	32003	No	2	Encrypted
	xsengine	32007	No	2	Encrypted

Audit Policy	Policy Status	Audited Actions	Audited Action Status	Audit Level	Users	Audited Objects
AUTH_AUDIT	Disabled	GRANT P...	Successful events	Critical	All users	ALL OBJE...
Admin Connects	Enabled	CONNECT...	All events	Info	GENERAL...	ALL OBJE...
CRYPTO_AUDIT	Disabled	ALTER PE...	All events	Emergency	All users	ALL OBJE...
FIREFIGHTER_DEV	Disabled	ALL ACTI...	All events	Emergency	DEVELOP...	ALL OBJE...
SCHEMA_AUDIT	Enabled	INSERT	All events	Info	All users	ALL OBJE...

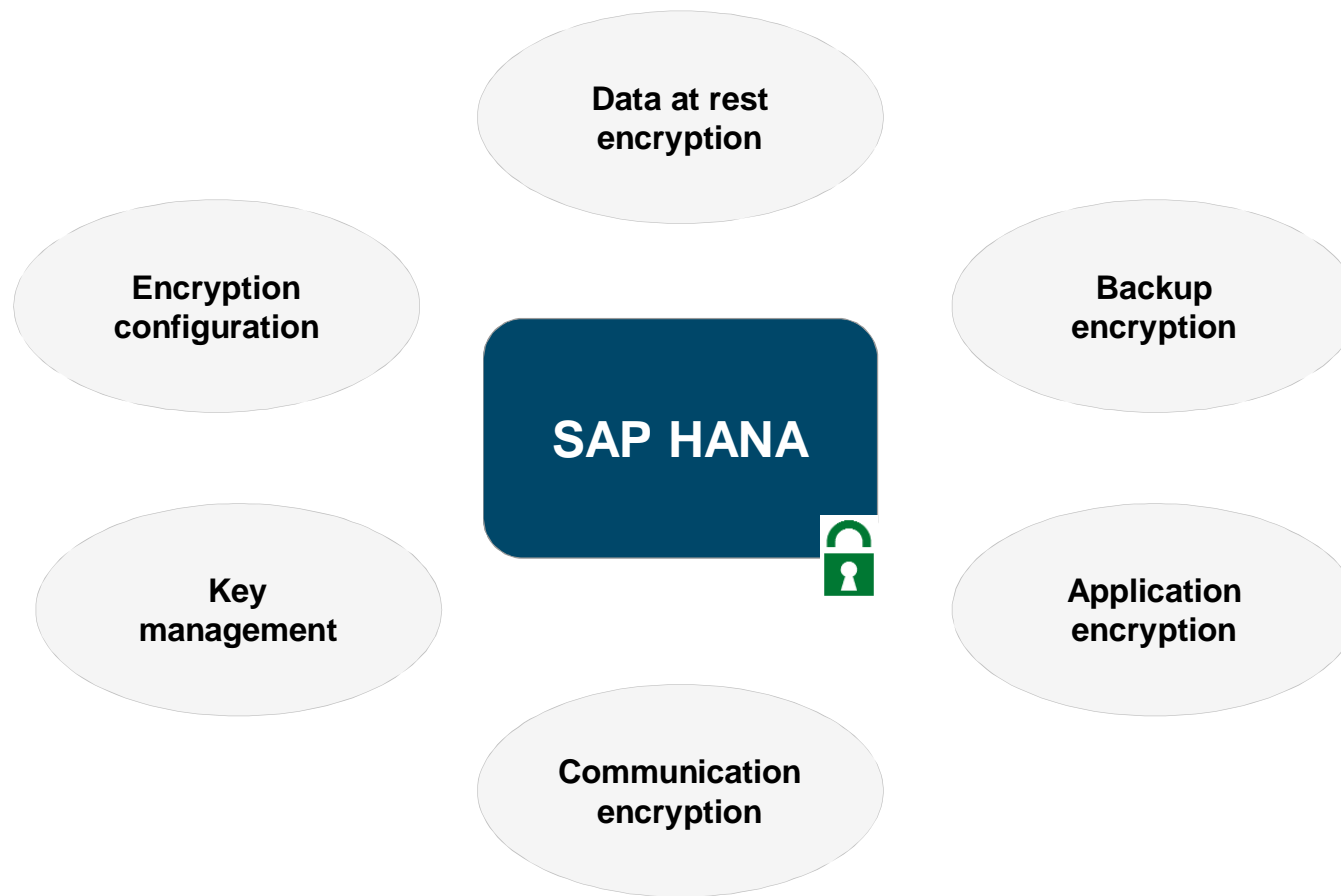
**Password Length and Composition**

- Minimum Password Length: 8
- Lowercase Letter Required: Yes
- Uppercase Letter Required: Yes
- Numerical Digit Required: Yes
- Special Character Required: No

**Password Lifetime**

- Lifetime of Initial Password: 7 days
- Minimum Password Lifetime: 1 day
- Maximum Password Lifetime: 182 days
- Maximum Duration of User Inactivity: 365 days
- Notification of Password Expiration: 14 days

# Comprehensive encryption



## Data at rest encryption

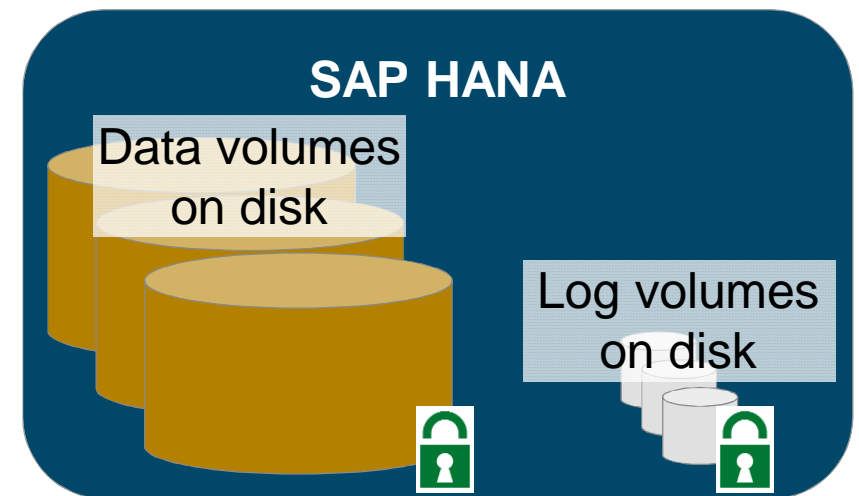
**Authorization is the primary means for fine-granular access control. Data at rest encryption is an additional layer of protection at the operating system level**

- § During operation, data is automatically saved from memory to disk at regular savepoints (data volumes)
- § Data changes are captured in redo log entries that are written to disk upon commit (log volumes)
- § Data and log volumes on disk are protected by file system permissions

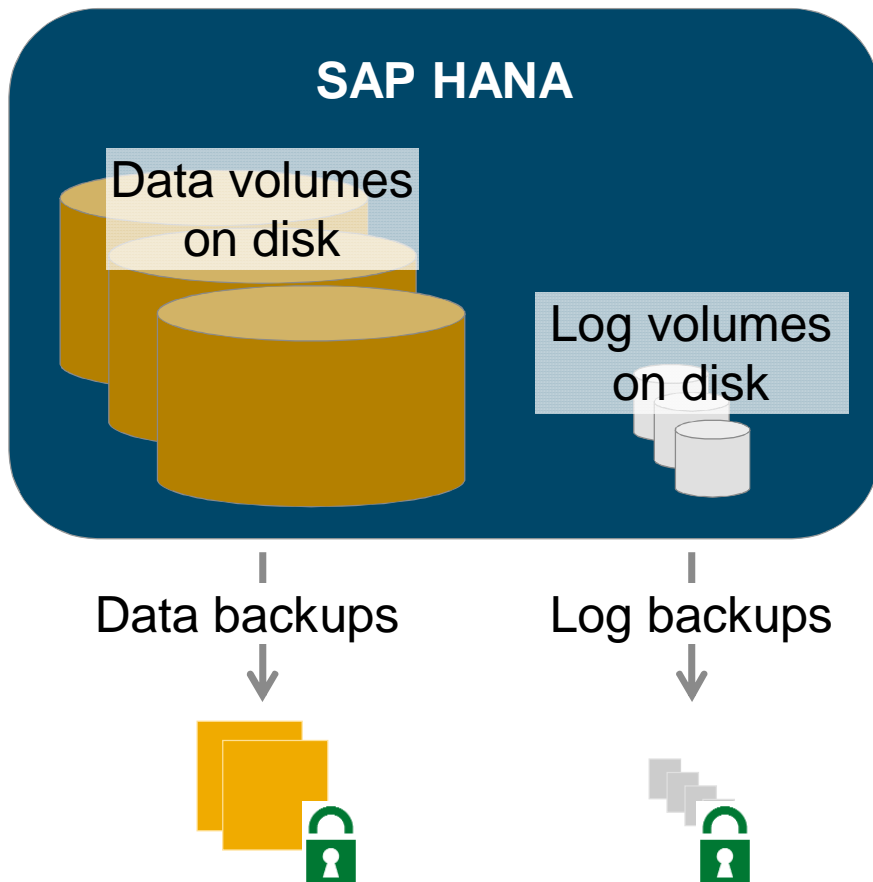
è Data volume encryption

è Redo log encryption

- § Enabling encryption does not increase database size on disk
- § SAP HANA uses SAP's standard cryptographic library ([FIPS-certified](#)).



# Backup encryption



## Backup encryption prevents unauthorized parties from accessing the content of backups

- § When backup encryption is active, all data backups and log backups are encrypted.
- § Both backups to file system and backups via the BACKINT interface can be encrypted. If you are using a third-party backup tool, you have a choice between native backup encryption or tool-side backup encryption.
- § Backup encryption is independent of the data volume and redo log encryption.
- § Note: Storage snapshots are not included in backup encryption. For encrypted storage snapshots you need to enable data volume encryption.

# Secure communication

## SAP HANA supports TLS/SSL connection encryption for network communication channels

- Y TLS/SSL for client-server communication (external channels) can be enforced
- Y Automatic setup of key management infrastructure (PKI) for internal communication channels

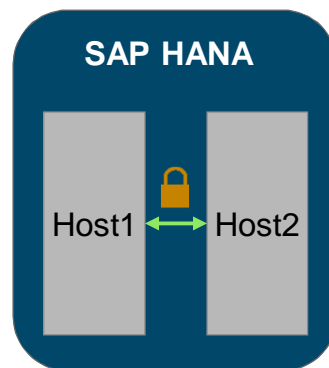
### External channels

### Internal channels

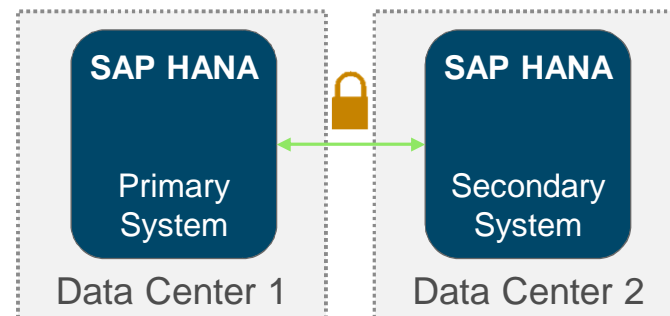
#### Client - server



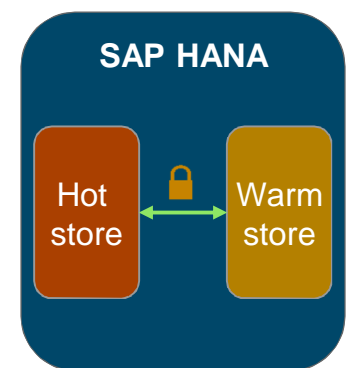
#### Scale-out system



#### System replication



#### + SAP option



# Network zones

## § Client zone

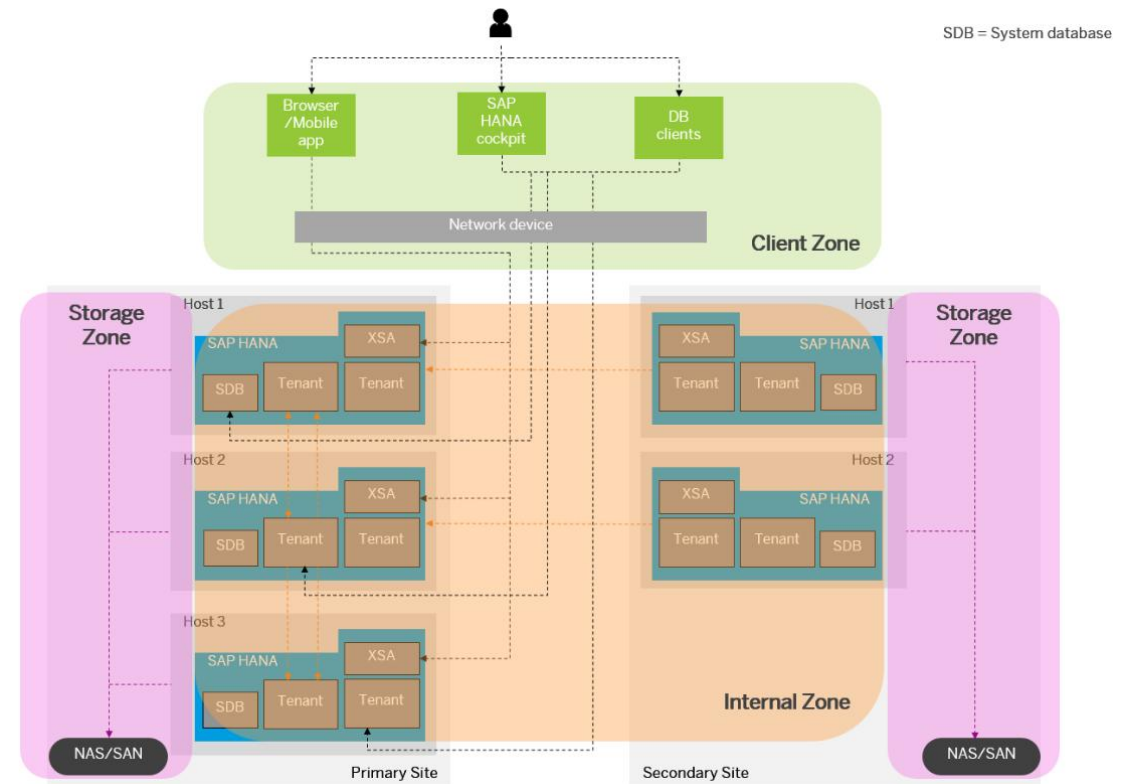
- SAP application servers, clients such as the SAP HANA studio or web applications running against the SAP HANA XS server, other data sources such as SAP Business Warehouse.

## § Internal zone

- Interhost network between hosts in a distributed system as well as the SAP HANA system replication network

## § Storage zone

- Network connections for backup storage and enterprise storage. In most cases, the preferred storage solution involves separate, externally attached storage subsystem devices that are capable of providing dynamic mount-points for the different hosts



XSC = SAP HANA extended application services, classic model

# Security infrastructure integration

## SAP HANA supports industry standards and documented interfaces to enable integration with the customers' security network and datacenter infrastructures

### § Identity management

- Connector for SAP Identity Management, SQL interface for integration with other identity management solutions
- Integration with LDAP for role assignment

### § Compliance

- Connector for SAP Access Control

### § Single Sign-On

- E.g. for Microsoft Active Directory

### § Logging

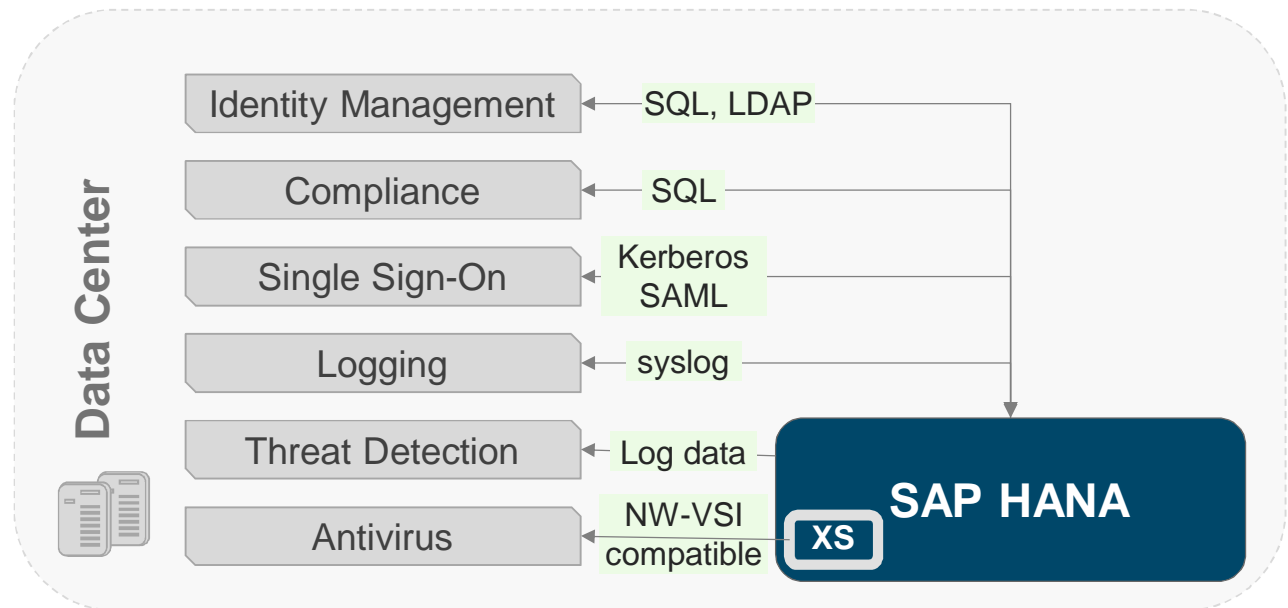
- Standard logging infrastructures (Linux syslog)

### § Threat detection

- SAP Enterprise Threat Detection support

### § Antivirus

- XS antivirus interface





# Recent innovations and roadmap



## Recent innovations – SAP HANA 2.0 SPS00/01

- ✓ Additional protection for sensitive and confidential data with **dynamic data masking**
- ✓ Protect your data at rest by using SAP HANA's comprehensive **encryption for data and redo log files and enhanced key lifecycle management**. Make sure that all your data and log backups are always encrypted by using **native backup encryption**
- ✓ Reduce TCO by using existing **LDAP groups for automatic role assignment**
- ✓ Increase application isolation, implement enhanced separation of duties and harden your security settings by leveraging the default **multi-container database mode**
- ✓ Simplified configuration and monitoring of security settings and user/role management in the **updated and extended SAP HANA cockpit**

# SAP HANA Platform Security Roadmap

## Recent innovations

### Data protection

- Dynamic data masking
- Native backup encryption
- Additional audit actions

### Simplification and TCO reduction

- New authentication option: JWT
- Password policy enhancements
- Catalog role editor in SAP HANA Cockpit
- Enhanced isolation, SoD and hardening features enabled by the default multi-container database mode

### Securing application scenarios

- XSA: JWT support, user propagation to services

## 2017 – Planned innovations

### Data protection

- User groups
- Audit logging enhancements

### Simple and secure operations

- Simplified encryption configuration and key management
- Additional security management capabilities in SAP HANA Cockpit
- Extended LDAP integration, e.g. nested groups
- SNI support

### Securing application scenarios

- SQLScript scanner
- XSA: Credential backup/restore

## 2018 – Product direction

### Data protection

- Extended encryption and key management, e.g. client-side column encryption
- Data masking extensions

### Simplification and TCO reduction

- Improved tool support for HDI-based roles in SAP HANA
- Extended LDAP integration, e.g. automatic user creation and LDAP authentication
- Additional security configuration and monitoring options in SAP HANA Cockpit

### Securing application scenarios

- XS Advanced: advanced security options, e.g. X.509 and SPNEGO authentication
- SDA: extend SSO to other remote sources, LDAP support extension for secondary credential

SAP HANA 2.0 SPS01

# Secure software, release strategy and patching



# SAP secure software development lifecycle

At the core of SAP's development processes is a comprehensive security strategy

## Secure software development lifecycle (secure SDL)



- § Comprehensive framework of processes, guidelines, tools and staff training
- § Ensures that security is an integral component of the architecture, design, and implementation of SAP solutions
- § Risk-based approach, uses threat-modeling and security risk assessment methods
- § Comprehensive security testing with automated and manual tests
- § See [SAP Security @ http://www.sap.com/security](http://www.sap.com/security)

# Security patches

**Keep up to date by installing the latest security patches and monitoring SAP security notes**

## Monthly SAP Security Patch Day

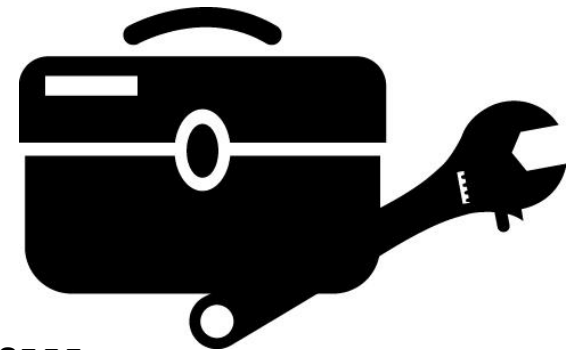
- SAP security notes contain information on the affected application areas and specific measures that protect against the exploitation of potential weaknesses
- See also <http://support.sap.com/securitynotes> and [SAP Security Notes – Frequently asked questions](#)

## Security improvements/corrections ship with SAP HANA revisions

- Installed using SAP HANA's lifecycle management tools
- See also SAP Note [2021789 – SAP HANA revision und maintenance strategy](#)

## Operating system patches

- Provided by the respective vendors SuSE/Redhat





# Security Patch Day – are my systems affected?

## 2424173 - Vulnerabilities in the user self-service tools of SAP HANA

Version 3 from 14.03.2017 in English

Description Software Components Support Package Patches This document is referenced by Attributes Languages

HANA XS classic, user self-service

### Reason and Prerequisites

User self-service tools is an application built on the SAP HANA extended application services, classic model (XS classic). It provides a web interface for features like password change, forgot password, etc. It is visible in the user interface nor configured in SAP HANA.

Only systems that have explicitly enabled the SAP HANA user self-service tools are affected by the vulnerabilities. More information on the SAP HANA user self-service tool is available in the SAP HANA documentation.

### Solution

The vulnerabilities have been fixed with revision 122.07 for SAP HANA 1.00 SPS 12 and revision 001 for SAP HANA 2.0 SPS 00. Update to these or later versions.

Alternatively, the user self-services can be deactivated if the service is not needed or as temporary workaround.

By default, the SAP HANA user self-service tool functionality is deactivated and the vulnerabilities cannot be exploited in this state.


To determine whether the SAP HANA user self-service tool is active, execute the following SQL query:

- SELECT NAME, STATUS FROM "\_SYS\_XS"."SQL\_CONNECTIONS" WHERE NAME = 'sap.hana.xs.selfService.user::selfService'

If the user self-service tool was activated (but not needed), you can deactivate it by deactivating the respective SQL connection artifact at

- http://<hostname>:80<xx>/sap/hana/xs/admin/#/package/sap.hana.xs.selfService.user/sqlcc/selfService or
- https://<hostname>:43<xx>/sap/hana/xs/admin/#/package/sap.hana.xs.selfService.user/sqlcc/selfService

More information about how to activate/deactivate SQL connection artifacts is available in the documentation: SAP HANA Administration Guide -> Maintaining the Application Services Run-Time Environment -> Maintaining the SAP HANA XS Classic Model Run Time -> Maintaining Application Runtime Configurations -> [Edit an SQL Connection Configuration](#).

 SAP HANA Blog

LoginUnited StatesContact Us

Search

Posts > Helping Customers Keep Their SAP HANA Systems Secure – Latest Security Updates

## Helping Customers Keep Their SAP HANA Systems Secure – Latest Security Updates

Posted by Holger Mack on March 13, 2017  
[More by this author >](#)

Tags: cybersecurity sap hana security

[Twitter](#) [Like](#) [Share](#) [37](#) [Share](#) [4](#)

In our previous [blog post](#) and on the SAP HANA security web site at <http://hana.sap.com/security>, we already described the comprehensive security approach that is applied at SAP and specifically at SAP HANA that helps customers to protect their most valuable assets.

One core element of SAP's security commitment is that SAP provides full transparency to customers on how they can set up, operate, and keep their systems secure.

As part of this commitment to transparency, with the latest [SAP Security Patch Day](#), on March 14<sup>th</sup>, 2017 SAP released five security notes for SAP HANA.

Of the five security notes, only two are rated with a Very High and High criticality. These criticality ratings indicate that affected customer systems could be at serious risk if an attacker exploits one of these vulnerabilities. Both issues affect only customers who:

- Are running on a specific version of the SAP HANA software, or
- Have enabled and exposed an optional component that is disabled by default

We expect very few SAP HANA customers to be affected by these issues. More details on these two issues are available in the "Technical Details" section at the end of this post.

Customers are specifically advised to assess if they are affected by either of these issues and take appropriate actions. SAP provides detailed information for security experts and administrators in the security notes listed below. Fixes for all issues are included in the newest supported releases of SAP HANA in line with SAP HANA's maintenance strategy.

If you want to learn more about SAP HANA security, read our [SAP HANA security whitepaper](#) or visit <http://hana.sap.com/security> for information on SAP's security strategy and approach, please visit <http://sap.com/security>.

**Additional Technical Details:**

Below is a short summary of the most important notes affecting SAP HANA customers (criticality very high and high). For information on all SAP security notes released as part of this SAP Security Patch Day, please go to [SAP Security Response Blog](#).

- Security note [2424173](#) (\*) is rated with a CVSS score of 9.8 (Very High) and can allow an attacker to take control of the system. However, this affects only customers if the optional User Self Service component (**disabled by default**) has been enabled and exposed to an untrusted network. The component is part of the SAP HANA extended application services, classic model. The security note contains instructions on how to check if the User Self Service tool is enabled and how to protect the system by either updating or deactivating the affected service (if not needed anymore or as temporary measure).
- Security note [2429069](#) (\*) is rated with a CVSS score of 8.8 (High) and could allow an attacker to elevate privileges by impersonating another user in the system. **This issue only affects systems running SAP HANA 2.0 SPS 00 revision 0 that expose SAP HANA extended application services, classic model to an untrusted network.**

# SAP HANA Maintenance Strategy

## Incremental, non-disruptive innovation

Updates and enhancements to the SAP HANA Platform will be released in the form of **SAP HANA Support Package Stacks twice per year**, delivered from within a single delivery stream.

- § As updates shipped for the SAP HANA Platform are strictly downward compatible, earlier revisions may be removed from SAP Service Marketplace with availability of a newer SAP HANA revision of the same SPS.
- § Incompatible changes may be considered for legal or security reasons, but are subject to a strict exception approval process.

The SAP HANA Platform product remains in maintenance as long as any SAP business application releases built on top of SAP HANA are in mainstream maintenance, extended maintenance, or priority-one support.

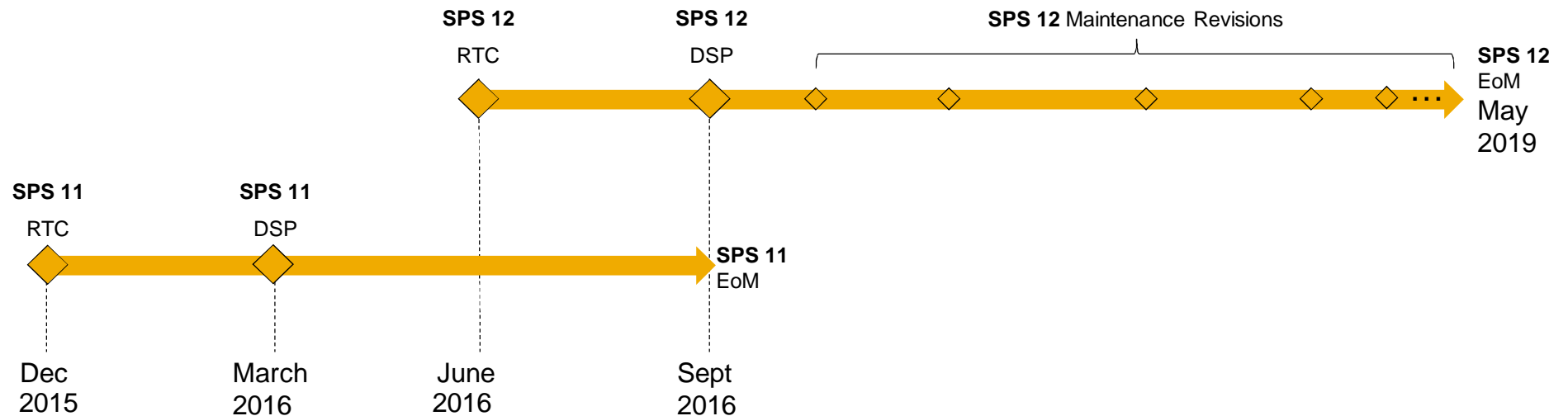


# SAP HANA Maintenance Strategy

## Revision Strategy for SPS12

For SAP HANA SPS12:

- SAP will provide Maintenance Revisions for a period of 3 years after SPS12 RTC
- There will be regular upgrade paths from SPS12 to any newer SPS

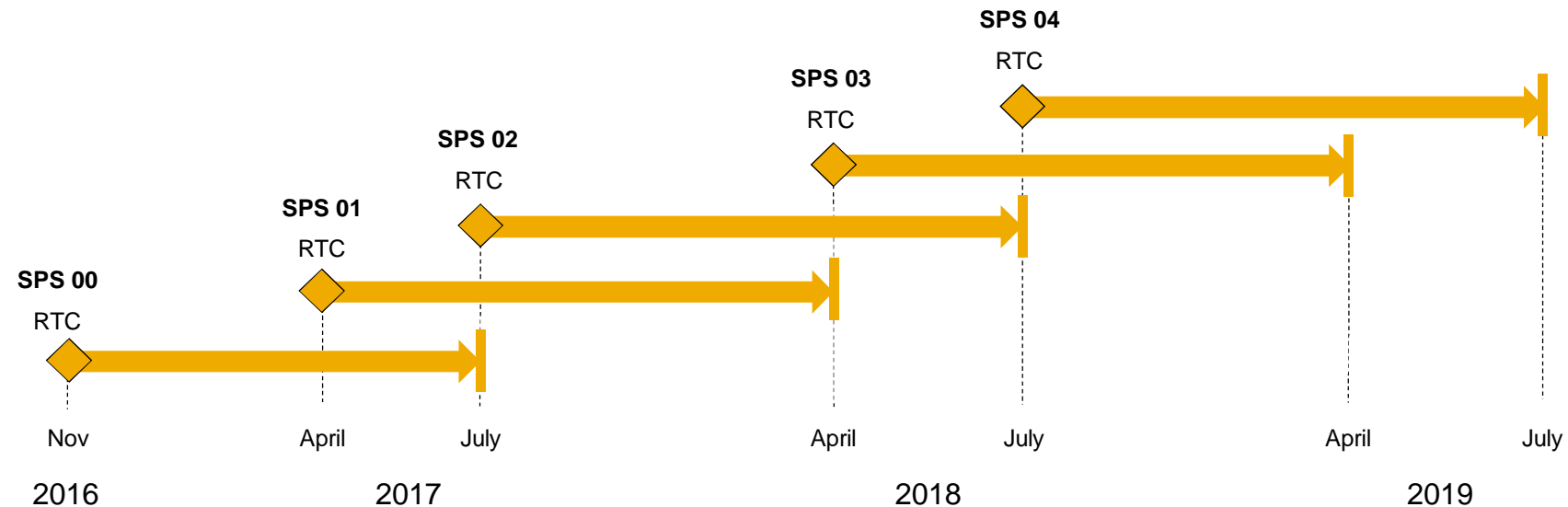


See SAP Note [2021789](#) for further details

# SAP HANA Maintenance Strategy

## Revision Strategy for SAP HANA 2.0

- § New capabilities are introduced **twice a year** in **SAP HANA Support Package Stacks (SPS)**
- § SAP is providing **bug fixes and security patches** for every SPS until the **SPS after next** is released
- § We recommend that maintenance timelines and project go live dates are adjusted to this release schedule



# SAP HANA Maintenance Strategy

## Upgrade to SAP HANA 2.0

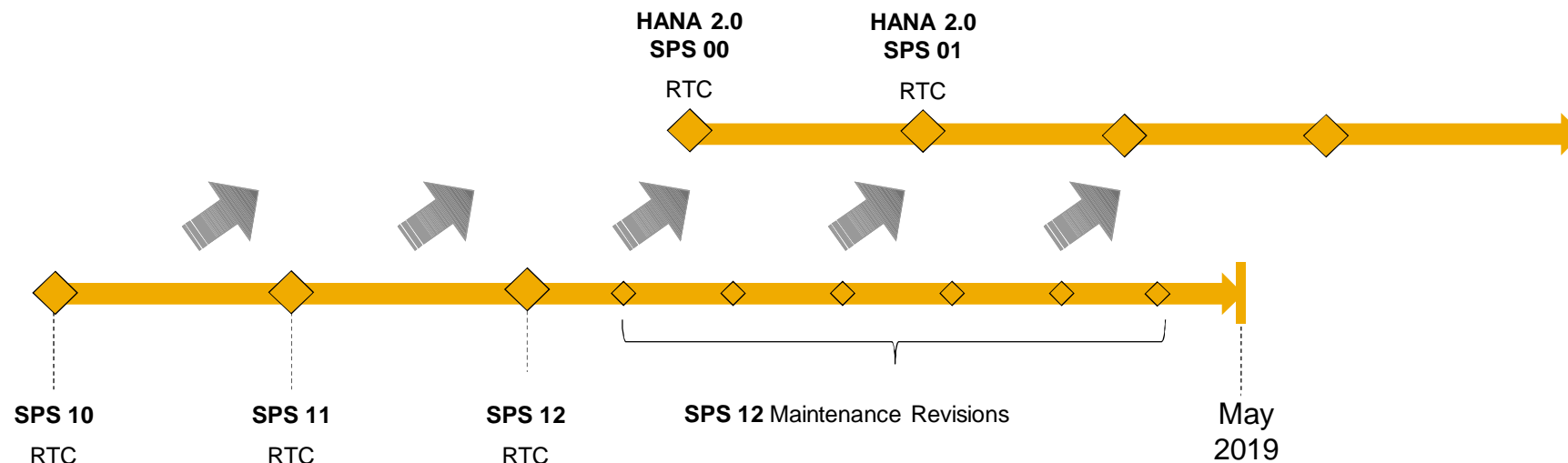
**Customers running mission critical systems might stay on SPS12 until May 2019**

§ SAP HANA 2.0 is upward compatible, customers just have to do a normal upgrade, no migration

**Upgrade from any SAP HANA system running on SPS10 or newer is possible**

§ Customers on SAP HANA SPS09 or lower first need to upgrade to a HANA SPS  $\geq$  SPS 10\*

However we recommend to first upgrade to the latest SPS12 revision before upgrading to SAP HANA 2.0 to be able to use Capture & Replay tool for regression tests



# SAP HANA Maintenance Strategy

## Overview SAP Notes

Support Package Stack	Start Revision	Revision as of Datacenter Service Point - DSP Revision (SAP production system verified SAP HANA Revision)	Last Revision in SPS (before switch to Maintenance Revision)	Last Available Maintenance Revision in SPS	
<a href="#">SAP HANA Platform SPS 06 Release Note 1848976</a>	<a href="#">SAP HANA Revision 60</a>	n.A.	<a href="#">SAP HANA Revision 69</a>	<a href="#">SAP HANA Revision 69.07 (final)</a>	
<a href="#">SAP HANA Platform SPS 07 Release Note 192167</a>	Support Package Stack		Last Released Revision	Last Revision in SPS (before switch to Maintenance Revision)	Last Available Maintenance Revision in SPS
<a href="#">SAP HANA Platform SPS 08 Release Note 200465</a>					
<a href="#">SAP HANA Platform SPS 09 Release Note 207526</a>					
<a href="#">SAP HANA Platform SPS 10 Release Note 216582</a>					
<a href="#">SAP HANA Platform SPS 11 Release Note 222746</a>					
	<a href="#">SAP HANA Platform 2.0 SPS 00 Release Note</a>	<a href="#">SAP HANA 2.0 SPS 00 Database Revision 000</a>	<a href="#">SAP HANA 2.0 SPS 00 Database Revision 002</a>	-	-
	<a href="#">SAP HANA Platform 2.0 SPS 01 Release Note</a>	<a href="#">SAP HANA 2.0 SPS 01 Database Revision 010</a>	<a href="#">SAP HANA 2.0 SPS 01 Database Revision 010</a>		
<a href="#">SAP HANA Platform SPS 12 Release Note 2298750</a>	<a href="#">SAP HANA Revision 120</a>	<a href="#">SAP HANA Revision 122</a>	SPS12 DSP Revision: <a href="#">SAP HANA Revision 122</a>	<a href="#">SAP HANA Revision 122.04</a>	

**SAP Note [2021789](#) (HANA 1.0)**  
**SAP Note [2378962](#) (HANA 2.0)**  
*(as of 2017-12-05)*

# Customer pain points with software updates

## Never touch a running system?

- § Potential negative effects of system changes
  - On general system behavior, e.g. performance
  - On modifications and custom coding
  - On attached systems, e.g. applications on top

## Why are updates/upgrades expensive?

- § Need test hardware
- § Need testers
- § Need test cases (close to production)
- § Need time for tests
- § Need downtime



# Making SAP HANA upgrades as painless as possible

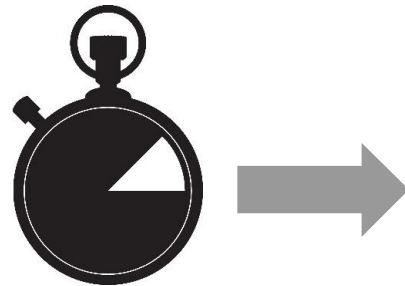
**Reduced testing effort**



**Capture and replay**

§ Run your production workload on a test system

**No/reduced downtime**



**Zero downtime maintenance**

§ Based on system replication

**Upgrade by moving tenants**

§ Based on multi-tenant database container scenario

# Capture and replay – testing revision upgrades





# Summary

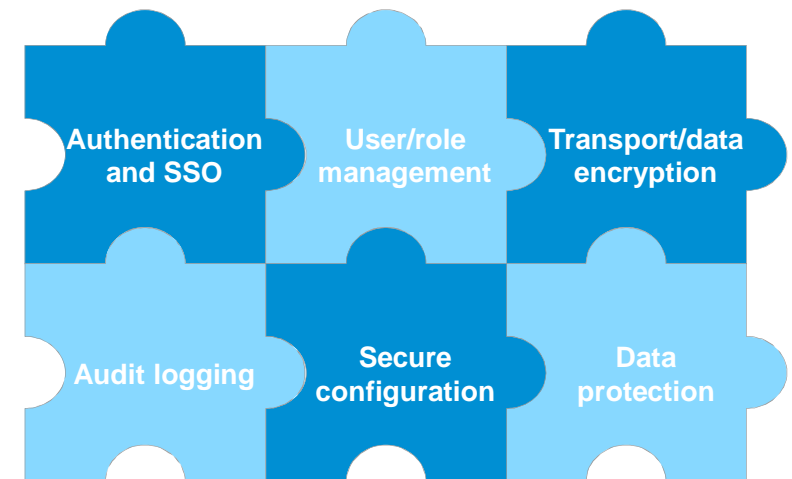




# Manage secure data access and keep your systems protected

## SAP HANA provides a comprehensive security framework

- ✓ Securely run SAP HANA in a variety of environments
- ✓ Meet increasing regulatory and compliance requirements
- ✓ Easily configure, manage and monitor security
- ✓ Keep up to date with relevant security updates



# Innovate with confidence on SAP HANA!

# More information



# More information on new security features in SAP HANA 2.0

## Documentation

§ [Release Notes](#)

§ [Updated documentation](#)

The screenshot shows the 'What's New in the SAP HANA Platform 2.0 (Release Notes)' document. It includes a table of contents on the left and a main content area with a table of support package stacks.

Support Package Stack (SPS)	First Released with Revision...	Release Note
00	2.00.000	SAP Note 2380257
01	2.00.010	SAP Note 2404375

The document also mentions that it accumulates features of all SAP HANA 2.0 support package stacks (SPS) and corresponding revisions, starting from revision 2.00.000 up to the current support package stack and revision.

## Blogs

§ [Enhanced Data Protection in SAP HANA 2.0 SPS 01](#)

§ [Protect your sensitive data using SAP HANA's new dynamic data masking](#)

§ [Multi-container database mode is the new default](#)

§ [LDAP Group Authorization](#)

The screenshot shows a blog post from the SAP HANA Blog. The title is 'Enhanced Data Protection in SAP HANA 2.0 SPS 01'. It was posted by Andrea Kristen on April 12, 2017. The post discusses the new security framework and tooling for authentication, authorization, and role management. It mentions that the new SAP HANA 2.0 SPS 01 release adds new features for enhanced protection of sensitive and confidential data, including dynamic data masking and native backup encryption.

The screenshot shows a community blog post from the SAP HANA Community. The title is 'Protect your sensitive data using SAP HANA's new dynamic data masking'. It was posted by Aleks Aleksic on April 12, 2017. The post discusses the new security framework and tooling for authentication, authorization, and role management. It mentions that the new SAP HANA 2.0 SPS 01 release adds new features for enhanced protection of sensitive and confidential data, including dynamic data masking and native backup encryption.

# Need more information on SAP HANA security?

Read the SAP HANA [security whitepaper](#)

2	Introduction.....	
2.1	What is SAP HANA?.....	
2.2	Deployment options .....	
2.3	Availability.....	
3	Scenarios .....	
3.1	Three-tier application .....	
3.2	Application on SAP HANA extended application services, cl.....	
3.3	Application on SAP HANA extended application services, ad.....	
3.4	Integrated scenario: reporting on ERP data in SAP HANA .....	
3.5	Integrated scenario: reporting on BW data in SAP HANA .....	
3.6	Data mart: customer-specific analytic reporting on SAP HAN.....	
4	Security functions .....	
4.1	Access control .....	
4.2	Secure configuration and encryption .....	
4.3	Tools and data center integration .....	13
5	Security in the software lifecycle .....	15
5.1	Secure development .....	15
5.2	Security patches .....	15



## SAP HANA Security Whitepaper

SAP HANA 2.0 SP1500  
Andreas Krielen, Holger Mack, Tim Schriener, Alois Altknecht (SAP SE)  
January 2017

Public

Check out our security website  
<http://hana.sap.com/security>

**Manage secure data access and protect your corporate information**

You need to meet the ever increasing cyber-security challenges, keep your systems secure, and stay on top of the compliance and regulatory requirements of today's digital world. You can run and operate SAP HANA securely in diverse environments, implementing your specific compliance, security, and regulatory requirements.

Find out information about important security updates for SAP HANA  
On the March 14th, 2017 SAP Security Patch Day, we released new security notes for SAP HANA. To find out more

## More information

### Documentation

#### [SAP Help Portal:](#)

- Security Guide, Administration Guide, Developer Guide, SQL Reference Guide

### Secure configuration guidelines

- [SAP HANA Security Checklists and Recommendations](#) are provided to accompany the detailed Security Guide
- [SAP Security Baseline Template](#)
- [DSAG Prüfleitfaden ERP 6.0](#) (by the German SAP user group)

### Whitepaper

- [SAP HANA Security Whitepaper](#)

### Best practices

- [How to Define Standard Roles](#)

### Training

- [HA 240](#)

### SAP Notes (login required)

- [2159014](#) FAQ: SAP HANA Security
- [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
- [784391](#) SAP support terms and 3rd-party Linux kernel drivers
- [1730999](#) Configuration changes in HANA appliance
- [863362](#) Security checks with SAP EarlyWatch Alert
- [2021789](#), [2378962](#) SAP HANA revision and maintenance strategy

# Vielen Dank

Contact information:

**Andrea Kristen, SAP**  
[andrea.kristen@sap.com](mailto:andrea.kristen@sap.com)