



---

# Advanced Concepts for Setting Up Security, Audit, and Compliance for SAP HANA

Ranjit Prithviraj, Managing Director, Fitch Ratings  
Sanjay Mahajan, Director, Fitch Ratings  
Session ID # ASUG84177

# About the Speakers

## Ranjit Prithviraj

- Managing Director, Fitch Ratings
- Responsible for global strategy and management of Enterprise applications for Fitch Group
- “Are we there yet”

## Sanjay Mahajan

- Director, Fitch Ratings
- Over 20 years of experience in SAP administration, security, databases including HANA, and various operating systems
- “Need to get a hobby other than Fitch and SAP”

# Key Outcomes/Objectives

1. As compared to the traditional databases, Additional skills are needed to secure SAP HANA databases
2. Specific clients connecting to HANA are secured differently
3. Auditing is not enabled by default, and should be explicitly enabled on all production systems

# Agenda

- **Fitch Overview**
- Traditional vs. HANA Database Security
- Security Administration
  - User and group administration
  - Privileges and Roles
- Tools –
  - HANA Studio,
  - HANA Cockpit
  - Web-based Development workbench
  - Command Line
  - SAP services/tools
- Auditing and Compliance
- OS and Network Security
- References and Important OSS notes

# Fitch Group

Fitch Group is a **global leader in financial information services** with operations in over 30 countries. Fitch Group is majority-owned by Hearst Corporation.

Fitch Ratings

Fitch Solutions

BMI Research

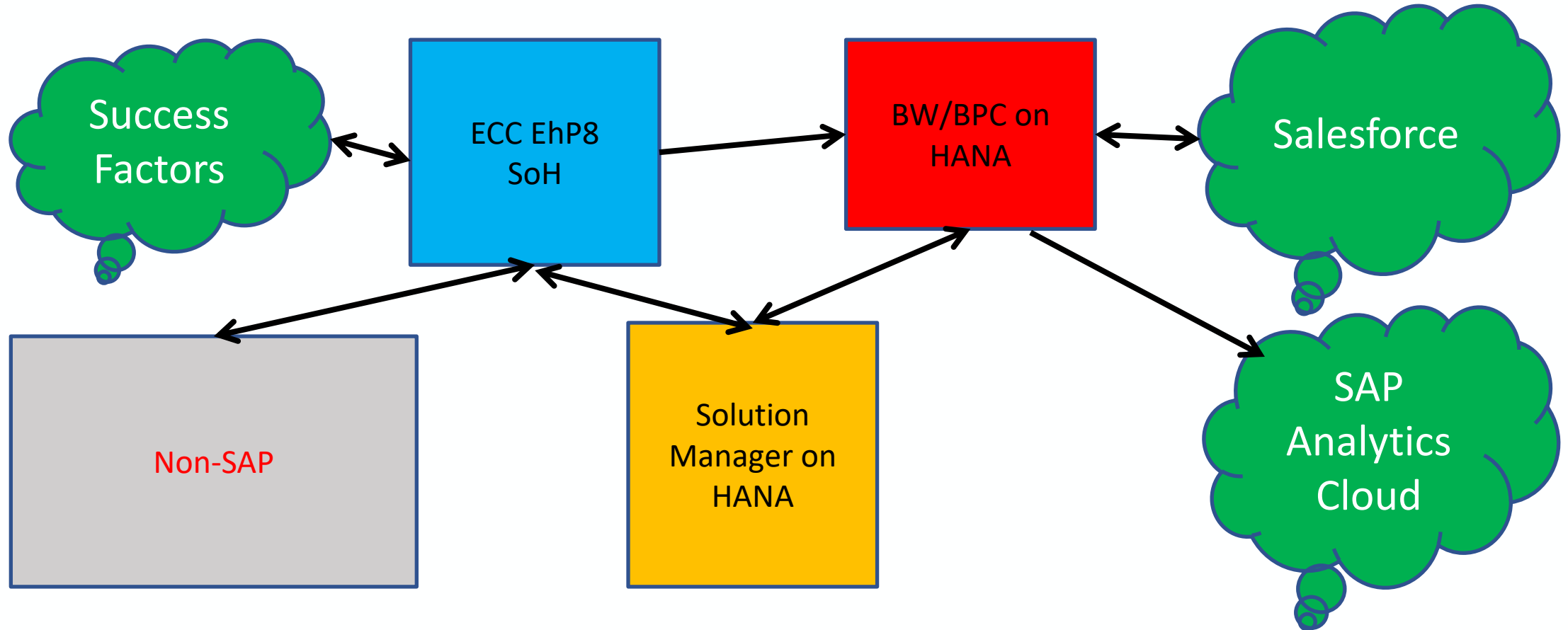
Fitch Learning

- One of the Big Three credit rating agencies
- Over \$1 Billion in revenue
- Over 4000 employees

**Dual headquarters in New York and London**

# Our SAP landscape

We use SAP for Finance, SD, MM, T&E, Reporting, and HR. It interfaces with several non-SAP applications



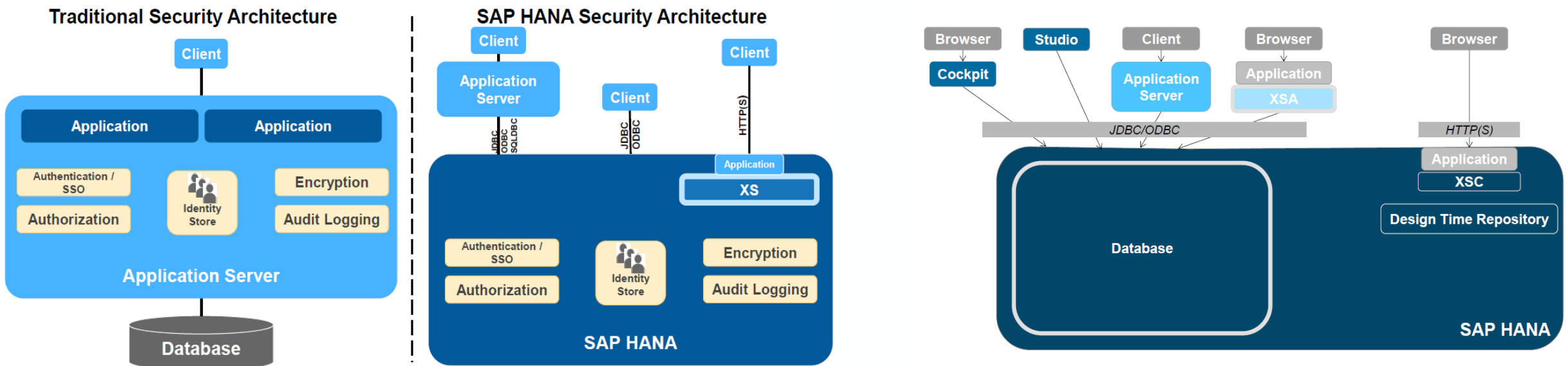
# Agenda

- Fitch Overview
- **Traditional vs. HANA Database Security**
- Security Administration
  - User and group administration
  - Privileges and Roles
- Tools –
  - HANA Studio,
  - HANA Cockpit
  - Web-based Development workbench
  - Command Line
  - SAP services/tools
- Auditing and Compliance
- OS and Network Security
- References and Important OSS notes

# Traditional vs. HANA Security Architecture

At its core, SAP HANA is a database, but it is more than just that: It's an application development environment, a multidimensional reporting system, a predictive analytics engine, and with S/4HANA, an OLTP engine. Comparatively, non-HANA databases only act as data store. Due to these differences, securing an SAP HANA DB system is much more complex than the traditional RDBMS databases.

## Security Architecture





# Agenda

- Fitch Overview
- Traditional vs. HANA Database Security
- **Security Administration**
  - User and group administration
  - Privileges and Roles
- Tools –
  - HANA Studio,
  - HANA Cockpit
  - Web-based Development workbench
  - Command Line
  - SAP services/tools
- Auditing and Compliance
- OS and Network Security
- References and Important OSS notes

# Types of Users

A user id is required to access the HANA database. There are two types of users – Standard users (Technical users or real people) and Restricted users

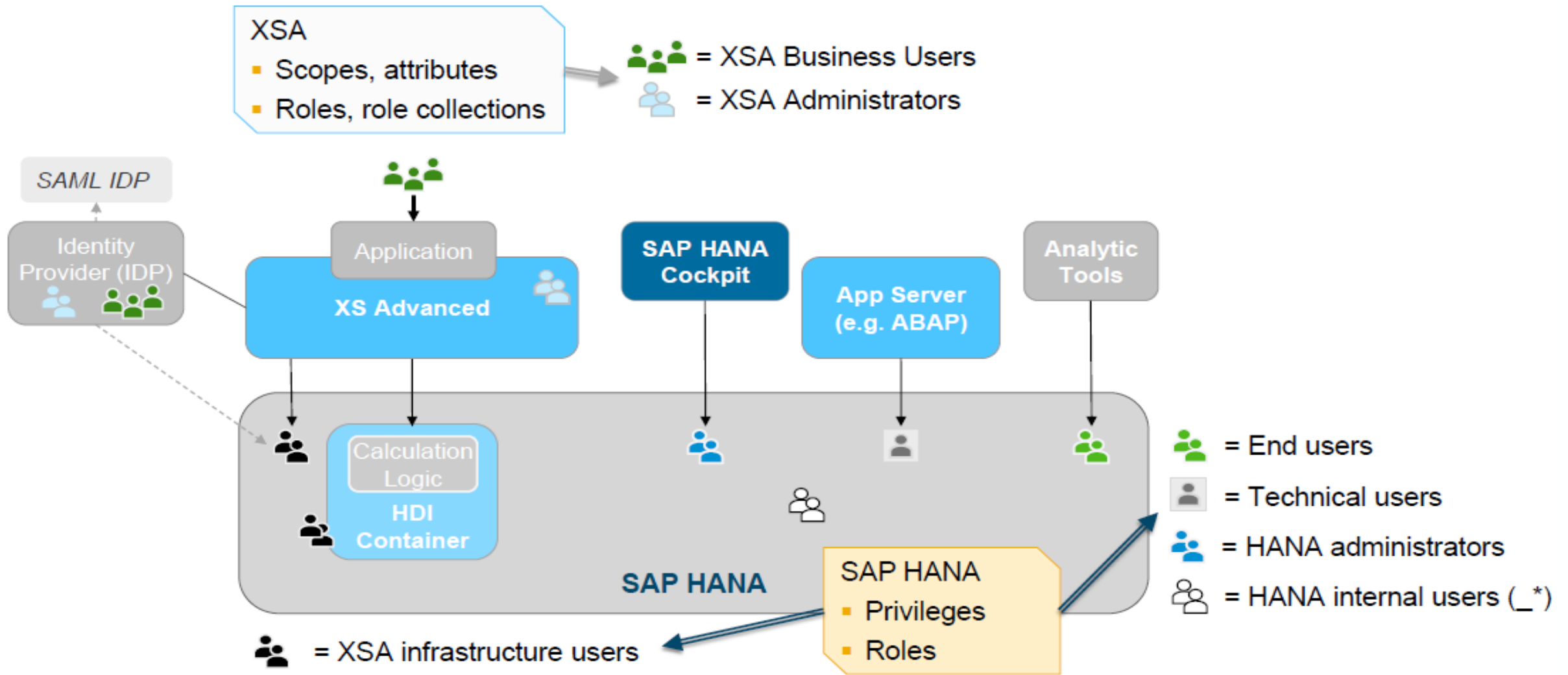
Standard		Restricted
Real users	Technical users	
The difference between real users and technical users is conceptual. Technically, they are same		Intended for provisioning users who access SAP HANA through client applications and who are not intended to have full SQL access
dropped if a person leaves the organization.	Examples: SYS and _SYS_REPO	Cannot create objects or view data
SQL connectivity, can create objects in their schema		HTTP connectivity

# Properties of users

```
select user_name, user_mode, creator, is_password_enabled, user_deactivated, IS_RESTRICTED from SYS.USERS where user_name like 'A%' or user_name like 'S%'
```

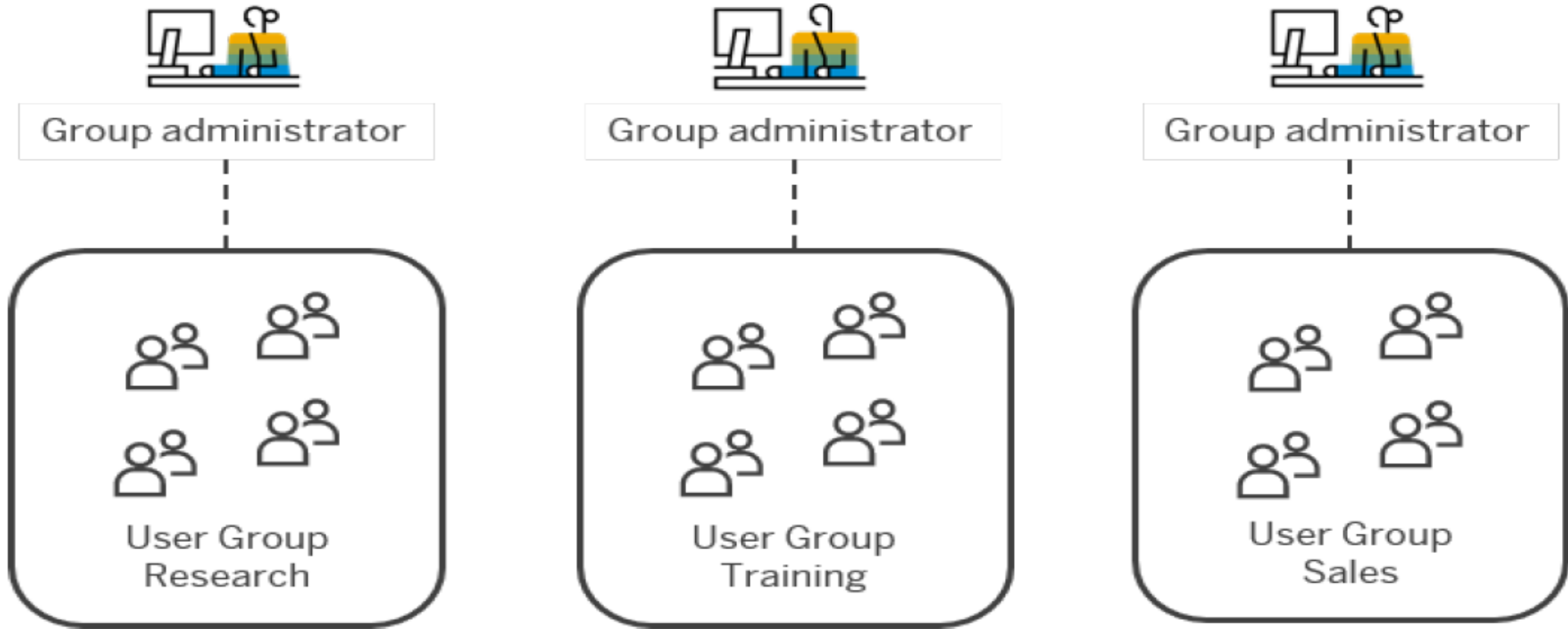
	USER_NAME	USER_MODE	CREATOR	IS_PASSWORD_ENABLED	USER_DEACTIVATED	IS_RESTRICTED
1	SYS	LOCAL	SYS	TRUE	TRUE	FALSE
2	SYSTEM	LOCAL	SYS	TRUE	FALSE	FALSE
3	SMAHAJ01	LOCAL	SYSTEM	TRUE	FALSE	FALSE
4	SAPEP2	LOCAL	SYSTEM	TRUE	FALSE	FALSE
5	A_RES_USER	LOCAL	SMAHAJ01	TRUE	FALSE	TRUE
6	A_REG_USER	LOCAL	SMAHAJ01	TRUE	FALSE	FALSE

# SAP HANA users



# User Groups

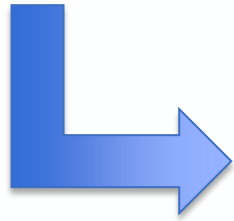
A user group can be configured for exclusive administration, which means that only the designated group administrator(s) can manage the users in the group. This could be useful, for example, to protect highly-privileged users or technical users from accidental deletion or manipulation.



User Groups

# Privileges and Roles

Privileges	Roles
Basic authorizations	Collection of privileges
Granted to user or role	Granted to user or role

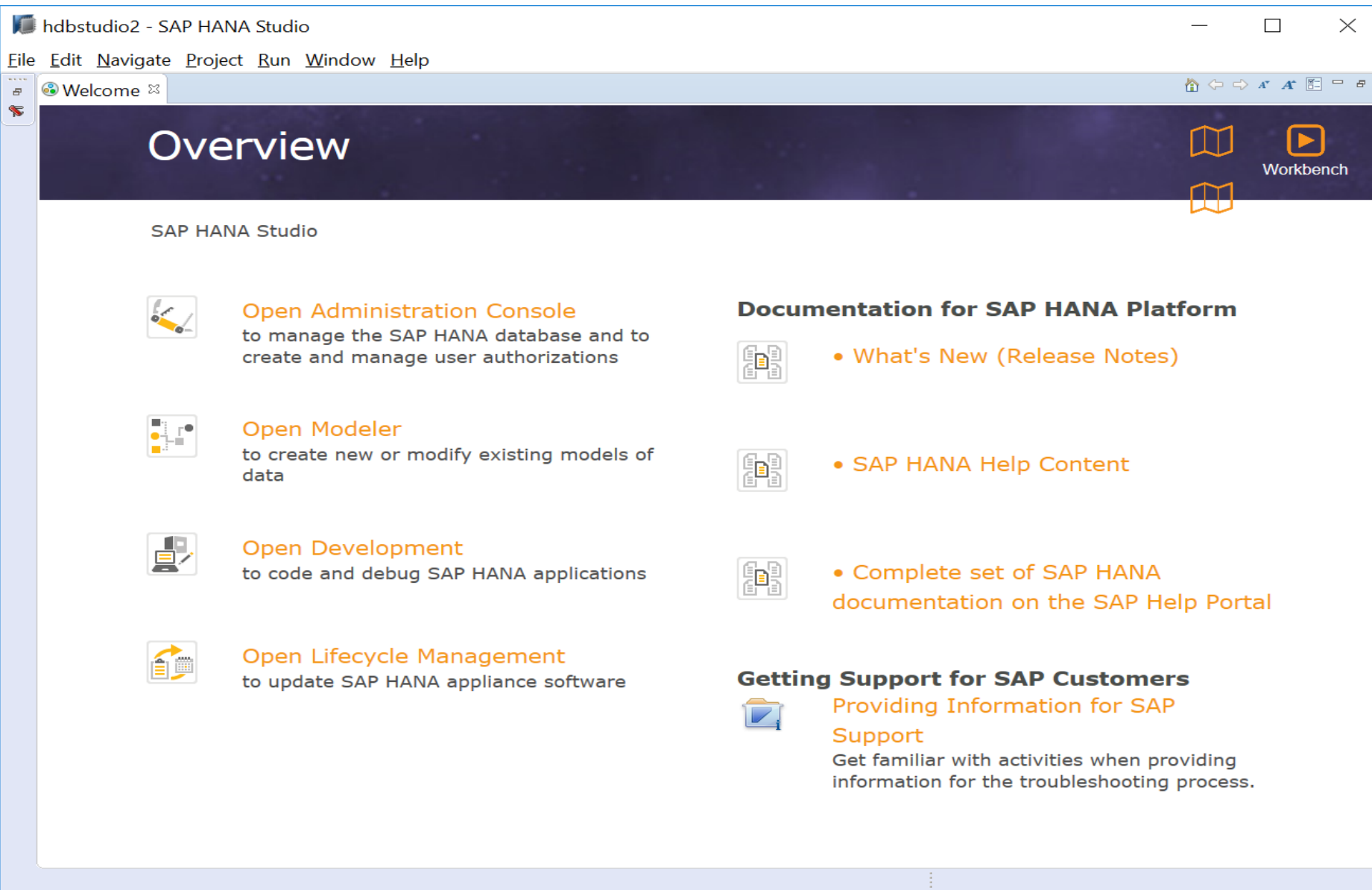


- ❖ **System Privilege** – Controls general system administration activities such managing schemas, users, roles, backups, stop/start databases etc.
- ❖ **Object Privilege** – Allows access to and modification of database objects such as tables and views. Depending on the object type, several actions can be authorized, such as CREATE, ALTER, DROP, SELECT etc.
- ❖ **Analytic Privilege** - Allows read access to data in SAP HANA information models (analytic views, attribute views, and calculation views) depending on certain values or combinations of values.
- ❖ **Package Privilege** - Allows access to and the ability to work in packages in the **classic repository** of the SAP HANA database. With SAP HANA **XS Advanced**, source code and web content are not versioned or stored in the SAP HANA database, so package privileges are not used in this context.
- ❖ **Application Privilege** - Developers of SAP HANA **XS Classic** applications can create application privileges to authorize user and client access to their application. With SAP HANA **XS Advanced**, application privileges are not used.
- ❖ **DEBUG Privilege** – A user can give ATTACH DEBUGGER privilege to another user

# Agenda

- Fitch Overview
- Traditional vs. HANA Database Security
- Security Administration
  - User and group administration
  - Privileges and Roles
- Tools –
  - HANA Studio,
  - HANA Cockpit
  - Web-based Development workbench
  - Command Line
  - SAP services/tools
- Auditing and Compliance
- OS and Network Security
- References and Important OSS notes

# HANA Studio



Eclipse-based environment for administration of SAP HANA databases and development of native SAP HANA applications.

- ▶ Initial administration tool for SAP HANA databases
- ▶ Built as a Java application
- ▶ **No longer in feature development**



# Create new user

hdbstudio2 - System: SYSTEMDB@EHS Host: sap-ehs-aue-001 Instance: 00 Connected User: SYSTEM System Usage: Custom System - SAP HANA Studio

File Edit Navigate Project Run Window Help

Systems Security SYSTEMDB@EHS (SYSTEM) Sandbox - SYSTEMDB

**Security SYSTEMDB@EHS (SYSTEM) Sandbox - SYSTEMDB** sap-ehs-aue-001 00

Auditing Password Policy SAML Identity Providers Data Volume Encryption

**System Settings for Auditing**

Global Settings

Auditing Status:  Audit Trail Target:   
Directory Name:

Audit Level Trail Targets

Audit Level	Audit Trail T...
CRITICAL	
EMERGENCY	
ALERT	

Audit Policies

Policy	Policy Stat...	Audited Actions	Audited Action Sta...	Audit Level	Users	Target Object	Audit Trail T...

Users

- New User
- New Restricted User
- Refresh F5
- Find User
- Filters...
- XSSQLCC\_AUTO\_USER\_D5D3B0C4F06A7...
- \_SYS\_AFL
- \_SYS\_EPM
- \_SYS\_REPO
- \_SYS\_STATISTICS
- \_SYS\_TASK
- \_SYS\_WORKLOAD\_REPLAY
- SYS XB

# Create new user

hdbstudio2 - New User System: SYSTEMDB@EHS Host: sap-ehs-aue-001 Instance: 00 Connected User: SYSTEM System Usage: Custom System - SAP ...

File Edit Navigate Project Run Window Help

Systems

Security SYSTEMDB@EHS \*SYSTEMDB@EHS - New User

SYSTEMDB@EHS (SYSTEM) Sandbox - SYSTEMDB sap-ehs-aue-001 00

User User Parameters

**New User**

User Name\*: USER1  Disable ODBC/JDBC access

Authentication

Password  SAML  SAP Logon Ticket

Password\*: ..... Confirm\*: ..... [Configure](#)

Force password change on next logon:  Yes  No  X509  SAP Assertion Ticket

Kerberos [Configure](#)

External ID\*: .....

Valid From: ..... Valid Until: .....

Session Client: .....

Granted Roles System Privileges Object Privileges Analytic Privileges Package Privileges Application Privileges Privileges on Users

# Create user in SU01

**Maintain Users**

User: TEST01  
Changed By: [ ] [ ] 00:00:00 Status: Not saved

Documentation | Address | Logon Data | DBMS | SNC | Defaults | Parameters | Roles

**Person**

Title: [ ]  
Last name: user  
First name: test  
Academic Title: [ ]  
Full Name: test user  
Language: [ ]

**Work Center**

Function: [ ]  
Department: [ ]  
Room Number: [ ] Floor: [ ] Building code: [ ]

**Communication**

Telephone: [ ] Extension: [ ]  
Mobile Phone: [ ]  
Fax: [ ] Extension: [ ]  
E-Mail Address: test01@company.com  
Method: E-Mail | Other Communication...

User: TEST01  
Changed By: [ ] [ ] 00:00:00 Status: Not saved

Documentation | Address | Logon Data | DBMS | SNC | Defaults | Parameters | Roles

Alias: [ ]

User Type: Dialog

Security Policy: [ ]

**Password**

New Password Rules (Case-Sensitive) [i]

New Password: [ ]  
Repeat Password: [ ]

Password Status: Initial Password (Set by Administrator) [i]

**User Group for Authorization Check**

User group: [ ]

**Validity Period**

Valid from: [ ]  
Valid To: [ ]

Ty... Message Text  
[ ] Password will be used for DBMS user

# Create user in SU01

User: TEST01  
Changed By: [ ] [ ] 00:00:00 Status: Not saved

Documentation | Address | Logon Data | **DBMS** | SNC | Defaults | Parameters | Roles | Profiles

**DBMS User**

DBMS User: TEST01  DBMS user does not exist

Valid from: [ ]

Valid To: [ ]

E-Mail Address: [ ]

Deactivated (Locked)  
 Restricted User

**Authentication**

Password  
New Password: [ ]  
Repeat Password: [ ]

Kerberos  
External Identity: [ ]

SAML  
 X509  
 SAP Logon Ticket  
 SAP Assertion Ticket

Ty... Message Text  
Password will be used for DBMS user

E1S@EHS (SYSTEM) E1S Database 10.128.34.129.00

User: User Parameters Deploy (F8)

**New User**

User Name\*: TEST01  Disable ODBC/JDBC access

**Authentication**

Password  
Password\*: [ ] Confirm\*: [ ]  
Force password change on next logon:  Yes  No

Kerberos  
External ID\*: [ ]

SAML  SAP Logon Ticket [Configure](#)

X509  SAP Assertion Ticket [Configure](#)

Valid From: [ ] Valid Until: [ ]

Session Client: [ ]

Granted Roles | System Privileges | Object Privileges | Analytic Privileges | Package Privileges | **Application Privileges** | Privileges on Users

Application Privilege	Grantor
-----------------------	---------

# HANA Cockpit 2.0

Web-based tool for **centralized** administration and monitoring of **multiple** SAP HANA 2.0 and SAP HANA 1.0 SPS 12 databases.

- ➔ Introduced in SAP HANA 2.0 SPS 00
- ➔ Absorbs functionality of SAP DB Control Center
- ➔ Built as an SAP HANA XS Advanced application
- ➔ SAPUI5 user interface
- ➔ Installed as a single stack, but does not require a dedicated instance of SAP HANA to operate

HANA Cockpit supports following security tasks –

- ➔ Monitor critical security settings
- ➔ Manage HANA users
- ➔ Auditing
- ➔ Data Encryption
- ➔ Manage client certificates
- ➔ Data anonymization

# HANA Cockpit Apps


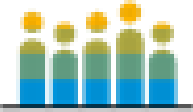


```
h4cadm@Cockpit host:/usr/sap/H4C/HDB96> xs apps
```

```
Getting apps in org "HANACockpit" / space "SAP" as COCKPIT_ADMIN...
```

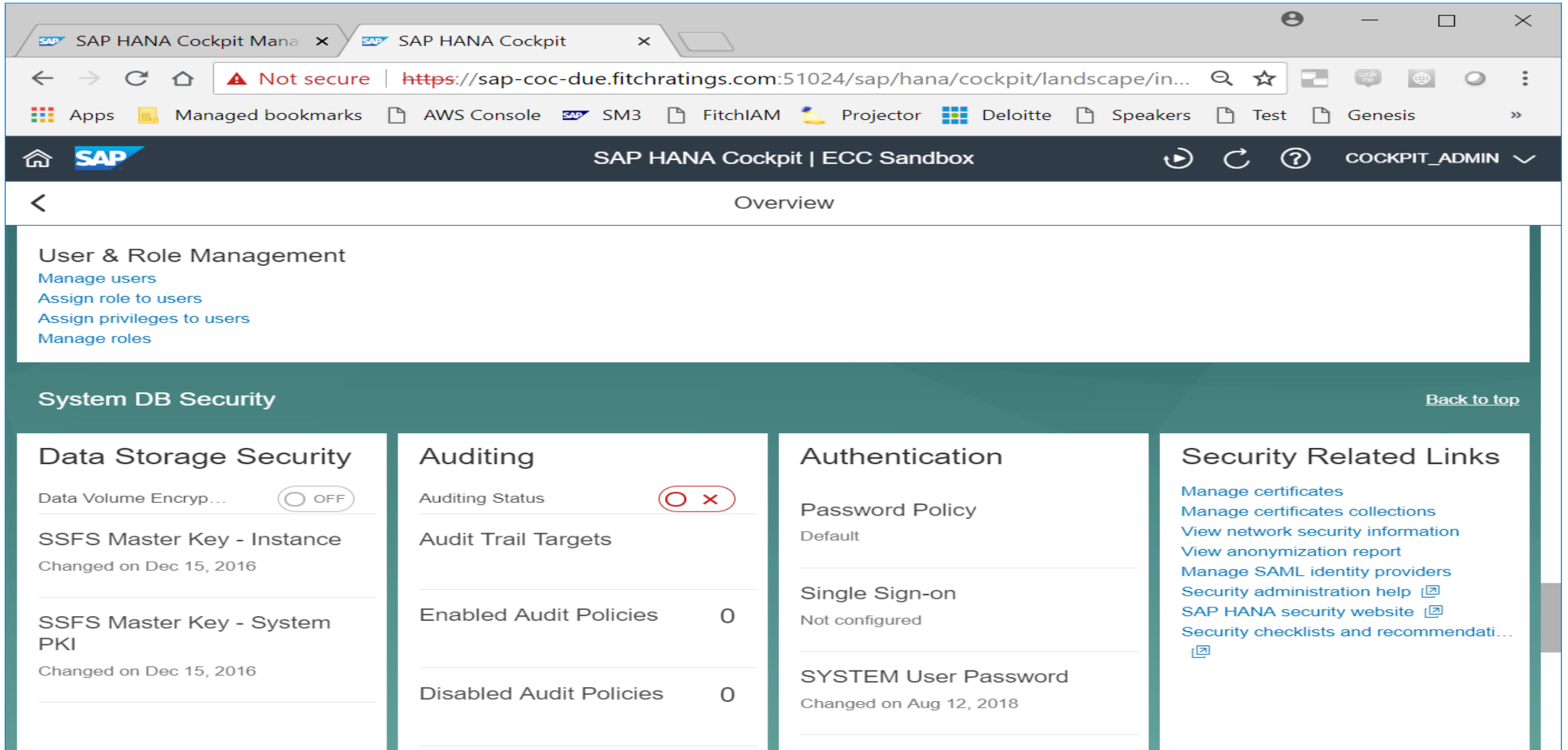
```
Found apps:
```

name	requested state	instances	memory	disk	urls
auditlog-db	STOPPED	0/1	16.0 MB	<unlimited>	<none>
auditlog-server	STARTED	1/1	256 MB	<unlimited>	https://<Cockpit host>:51002
auditlog-broker	STARTED	1/1	64.0 MB	<unlimited>	https://<Cockpit host>:51003
deploy-service	STARTED	1/1	280 MB	<unlimited>	https://<Cockpit host>:51004
component-registry-db	STOPPED	0/1	16.0 MB	<unlimited>	<none>
product-installer	STARTED	1/1	256 MB	<unlimited>	https://<Cockpit host>:51005
auditlog-odata	STARTED	1/1	128 MB	<unlimited>	https://<Cockpit host>:51007
auditlog-ui	STARTED	1/1	64.0 MB	<unlimited>	https://<Cockpit host>:51008
hrtt-service	STARTED	1/1	512 MB	<unlimited>	https://<Cockpit host>:51009
sqlanz-svc	STARTED	1/1	256 MB	<unlimited>	https://<Cockpit host>:51010
sqlanz-ui	STARTED	1/1	128 MB	<unlimited>	https://<Cockpit host>:51011
hrtt-core	STARTED	1/1	512 MB	<unlimited>	https://<Cockpit host>:51012
sapui5_fesv3	STARTED	1/1	256 MB	<unlimited>	https://<Cockpit host>:51015
xsa-cockpit	STARTED	1/1	512 MB	<unlimited>	https://<Cockpit host>:51016
cockpit-persistence-svc	STARTED	1/1	1.00 GB	<unlimited>	https://<Cockpit host>:51020
cockpit-hdb-svc	STARTED	1/1	768 MB	<unlimited>	https://<Cockpit host>:51021
cockpit-xsa-svc	STARTED	1/1	768 MB	<unlimited>	https://<Cockpit host>:51027
cockpit-collection-svc	STARTED	1/1	768 MB	<unlimited>	https://<Cockpit host>:51017
cockpit-hdbui-svc	STARTED	1/1	128 MB	<unlimited>	https://<Cockpit host>:51023
cockpit-telemetry-svc	STARTED	1/1	768 MB	<unlimited>	https://<Cockpit host>:51028
cockpit-landscape-svc	STARTED	1/1	128 MB	<unlimited>	https://<Cockpit host>:51022
cockpit-web-app	STARTED	1/1	512 MB	<unlimited>	https://<Cockpit host>:51024
cockpit-adminui-svc	STARTED	1/1	128 MB	<unlimited>	https://<Cockpit host>:51025
cockpit-admin-web-app	STARTED	1/1	128 MB	<unlimited>	https://<Cockpit host>:51026

# HANA Cockpit Set up

	Cockpit administrators
	Cockpit users
	Cockpit resources
	Cockpit configuration

# HANA Cockpit Security



The screenshot shows the SAP HANA Cockpit Security Overview page. The browser address bar indicates the URL is <https://sap-coc-due.fitchratings.com:51024/sap/hana/cockpit/landscape/in...>. The page title is "SAP HANA Cockpit | ECC Sandbox" and the user is logged in as "COCKPIT\_ADMIN".

The main content area is titled "Overview" and contains the following sections:

- User & Role Management**
  - [Manage users](#)
  - [Assign role to users](#)
  - [Assign privileges to users](#)
  - [Manage roles](#)
- System DB Security** (with a [Back to top](#) link)
  - Data Storage Security**
    - Data Volume Encryp...  OFF
    - SSFS Master Key - Instance**  
Changed on Dec 15, 2016
    - SSFS Master Key - System PKI**  
Changed on Dec 15, 2016
  - Auditing**
    - Auditing Status  **X**
    - Audit Trail Targets
    - Enabled Audit Policies: 0
    - Disabled Audit Policies: 0
  - Authentication**
    - Password Policy: Default
    - Single Sign-on: Not configured
    - SYSTEM User Password: Changed on Aug 12, 2018
  - Security Related Links**
    - [Manage certificates](#)
    - [Manage certificates collections](#)
    - [View network security information](#)
    - [View anonymization report](#)
    - [Manage SAML identity providers](#)
    - [Security administration help](#)
    - [SAP HANA security website](#)
    - [Security checklists and recommendati...](#)



# Web-based Development Workbench

<http://<hostname>:8000/sap/hana/ide/>

The screenshot shows a web browser window with the URL `sap-ehs-aue-001:8000/sap/hana/ide/`. The browser's address bar and tabs are visible. The main content area of the browser displays the SAP HANA Web-based Development Workbench interface. At the top of the interface is a blue header with the SAP logo and the text "SAP HANA Web-based Development Workbench". Below the header, the main content area features the title "SAP HANA Web-based Development Workbench" in a large, bold font. Underneath the title, there are four blue rectangular buttons, each with an icon and a description of its function:

- Editor**: Represented by a pen icon. Description: "Create, edit, execute, debug and manage HANA Repository artifacts".
- Catalog**: Represented by a database icon. Description: "Create, edit, execute and manage HANA DB SQL catalog artifacts".
- Security**: Represented by a shield icon. Description: "Create users, create roles, assign objects and manage security".
- Traces**: Represented by a circular icon with a gear. Description: "View, download traces for HANA applications, set trace levels".

# Web-based Development Workbench – Direct links

module	link	role
Editor	<a href="http://&lt;WebServerHost&gt;:80&lt;SAPHANAinstance&gt;/sap/hana/xs/ide/editor">http://&lt;WebServerHost&gt;:80&lt;SAPHANAinstance&gt;/sap/hana/xs/ide/editor</a>	sap.hana.xs.ide.roles::EditorDeveloper
Catalog	<a href="http://&lt;WebServerHost&gt;:80&lt;SAPHANAinstance&gt;/sap/hana/xs/ide/catalog">http://&lt;WebServerHost&gt;:80&lt;SAPHANAinstance&gt;/sap/hana/xs/ide/catalog</a>	sap.hana.xs.ide.roles::CatalogDeveloper
Security	<a href="http://&lt;WebServerHost&gt;:80&lt;SAPHANAinstance&gt;/sap/hana/xs/ide/security">http://&lt;WebServerHost&gt;:80&lt;SAPHANAinstance&gt;/sap/hana/xs/ide/security</a>	sap.hana.xs.ide.roles:: SecurityAdmin
Trace	<a href="http://&lt;WebServerHost&gt;:80&lt;SAPHANAinstance&gt;/sap/hana/xs/ide/trace">http://&lt;WebServerHost&gt;:80&lt;SAPHANAinstance&gt;/sap/hana/xs/ide/trace</a>	sap.hana.xs.ide.roles::TraceViewer

# Web-based Development Workbench - Security

The screenshot displays the SAP HANA Web-based Development Workbench: Security interface. The browser address bar shows the URL `sap-ehs-aue-001:8000/sap/hana/ide/security/`. The page title is "SAP HANA Web-based Development Workbench: Security" and the version is "v 1.120.20". The user is logged in as "USER: SMAHAJ01".

The interface is divided into several sections:

- Left Navigation Panel:** Lists various system roles and users, including `XSSQLCC_AUTO_USER_0E24920E`, `XSSQLCC_AUTO_USER_D5D3B0C`, `_SYS_AFL`, `_SYS_EPM`, `_SYS_REPO`, `_SYS_STATISTICS`, `_SYS_TASK`, `_SYS_WORKLOAD_REPLAY`, `_SYS_XB`, and a "Roles" section with roles like `AFLPM_CREATOR_ERASER_EXEC`, `AFLPM_ONLINE_REGISTRATION_E`, `AFL__SYS_AFL_ERPA_EXECUTE`, `CONTENT_ADMIN`, `MODELING`, `MONITORING`, `PUBLIC`, `RESTRICTED_USER_JDBC_ACCES`, `RESTRICTED_USER_ODBC_ACCE`, `sap.bc.ina.service.v2.userRole::INA_l`, `sap.hana.admin.cockpit.sysdb.roles::`, `sap.hana.admin.cockpit.sysrep.roles::`, and `sap.hana.admin.roles::Administrator`.
- User Configuration Panel (SMAHAJ01):**
  - User Parameters:** Includes fields for Password, Confirm, Kerberos External ID, Valid From (Aug 13, 2018 1:53:21 AM UTC-04:00), Valid Until, and Session Client.
  - Application Role Collections:** Includes checkboxes for SAML, SAP Logon Ticket, X509, and SAP Assertion Ticket, each with a "Configure" link.
- Granted Roles Panel:** Shows a table of roles granted to the user, with a "Details" button and a "Display" count of 8.

Role	Grantor
AFLPM_CREATOR_ERASER_EXECUTE	SYSTEM
AFLPM_ONLINE_REGISTRATION_EXECUTE	SYSTEM
AFL__SYS_AFL_ERPA_EXECUTE	SYSTEM
AFL__SYS_AFL_ERPA_EXECUTE_WITH_GRANT_OPTION	SYSTEM
CONTENT_ADMIN	SYSTEM

Assign authorization on Granted Roles in order to control by whom objects can be modified

# Command Line

Option	Action
Log onto a database in a single-container system	Run the following command all on one line: <pre>hdbsql -n &lt;host&gt; -i &lt;instance&gt; -u &lt;database_user&gt; - p &lt;database_user_password&gt;</pre>
Log onto a database in a multitenant database container	Run the following command all on one line: <pre>hdbsql -n &lt;host&gt; -i &lt;instance&gt; -u &lt;database_user&gt; - p &lt;database_user_password&gt; -d &lt;database_name&gt;</pre>

```
ehsadm@sap-ehs-aue-001:/usr/sap/EHS/home> hdbsql -n sap-ehs-aue-001:30041
```

Welcome to the SAP HANA Database interactive terminal.

Type: \h for help with commands

\q to quit

hdbsql=>

Single Sign-On authentication failed

Username: system

Password:

# Command Line – Create user

```
hdbsql E1S=> create user test1 password Welcome1  
0 rows affected (overall time 13.590 msec; server time 10.923 msec)
```

```
ehsadm@sap-ehs-aue-001:/usr/sap/EHS/home> hdbsql -n sap-ehs-aue-001:30041 -u system -p Sapphire19  
"create user test2 password Welcome1"  
0 rows affected (overall time 11.092 msec; server time 9982 usec)
```

```
ehsadm@sap-ehs-aue-001:/usr/sap/EHS/home> cat command_file
```

```
create user test3 password Welcome1;
```

```
ehsadm@sap-ehs-aue-001:/usr/sap/EHS/home> hdbsql -n sap-ehs-aue-001:30041 -u system -p Sapphire19 -l  
command_file
```

```
ehsadm@sap-ehs-aue-001:/usr/sap/EHS/home>
```

```
Alter user user1 reset connect attempts;
```

```
Alter user user1 force password change;
```

# Hdbuserstore – appendix

The secure user store (hdbuserstore) is a tool installed with the SAP HANA client. It is used to store connection information to SAP HANA systems securely on the client.

This allows the client applications to connect to SAP HANA without having to enter this information. It is typically used by scripts connecting to SAP HANA.

The secure user store can only be used for SQLDBC and JDBC-based connections. The SAP HANA studio does not use the SAP HANA secure user store, but instead uses Eclipse secure storage.

The secure user store is installed with the SAP HANA client package. After you install the client, the hdbuserstore program can be found in /usr/sap/hdbclient (Linux)

Connection information in the secure store is saved in the file SSFS\_HDB.DAT.

```
e1sadm > hdbuserstore -i set BACKUPE1S  
<hostname>:30041 SYSTEM TechEd18
```

```
e1sadm > hdbuserstore list  
DATA FILE    : /home/e1sadm/.hdb/e1s-aue-  
001/SSFS_HDB.DAT  
KEY FILE     : /home/e1sadm/.hdb/e1s-aue-  
001/SSFS_HDB.KEY
```

```
KEY BACKUPE1S  
  ENV : sap-ehs-aue-001:30041  
  USER: SYSTEM  
KEY DEFAULT  
  ENV : sap-ehs-aue-001:30041  
  USER: SAPEP2  
e1s-aue-001:e1sadm 5>
```

# SAP Provided Services/tools



EarlyWatch Alert  
Security Chapter

Checks on the most critical  
security requirements.



Security  
Optimization Service  
(SOS)

Detailed assessment on  
secure configuration and  
operation topics.



System  
Recommendations

Support for the selection  
and implementation of  
SAP Security Notes.



Configuration  
Validation on  
Security

Verifying SAP landscapes  
for compliance to Security  
Baselines and Policies.



Security in the  
Monitoring and  
Alerting  
Infrastructure

Monitoring and Alerting on  
security-critical events and  
properties.

The goal of these tools and services is to compare the customer's systems with SAP's security best practices and provide recommendations.

# Agenda

- Fitch Overview
- Traditional vs. HANA Database Security
- Security Administration
  - User and group administration
  - Privileges and Roles
- Tools –
  - HANA Studio,
  - HANA Cockpit
  - Web-based Development workbench
  - Command Line
  - SAP services/tools
- **Auditing and Compliance**
- OS and Network Security
- References and Important OSS notes



# Auditing

Set up rules to record and track specific changes made within the SAP HANA system, such as –

- Changes to user privilege and role definitions
- Failed logon attempts
- Changes to database configuration
- Access to sensitive data
- Highly privileged users

By default, SAP HANA auditing is not enabled, nor are systems configured to capture specific events within SAP HANA.

How to enable auditing -

- In HANA Studio, on the **Auditing** tab enable auditing, change the **Auditing Status:** dropdown option to **Enabled**.
- In the **Audit Trail Target:** dropdown, choose **Syslog (Default)**, **Database Table**, or **CSV Text File**
- When defining an audit rule, its audit level can be classified as **Emergency**, **Critical**, **Alert**, **Warning**, or **Info**.

# Auditing Policies

No custom audit policies are included out of the box. Audit policies can be defined to track specific events based on specific conditions. They're defined by an audit administrator based on the requirements of the organization. An audit policy is comprised of an audit action, audit action status, audit level, target object, target user, and trail target.

## An audit policy specifies which actions should be audited



- Create as few policies as possible
- Audit DML only if needed, as they have the biggest potential for performance impact
- Use security console to create/update policies and do not directly edit .ini files

# Compliance

- Do not use generic accounts unless absolutely necessary
- Lock SYSTEM user id and create separate administrator accounts
- Restrict access to the critical roles (be ready to provide justification)
- Create a separate BACKUP\_ADMIN account for running backups
- Encrypt data-at-rest if required
- Secure technical accounts for SAP applications
- Secure XSSQLCC\_AUTO\_USER\* accounts
- Set appropriate password policy (consistent with your company policy), for example see the table below.

force_first_password_change	true
last_used_passwords	12
minimum_password_lifetime	1
maximum_password_lifetime	90
minimal_password_length	8
password_layout	A1a
maximum_invalid_connect_attempts	6

# Agenda

- Fitch Overview
- Traditional vs. HANA Database Security
- Security Administration
  - User and group administration
  - Privileges and Roles
- Tools –
  - HANA Studio,
  - HANA Cockpit
  - Web-based Development workbench
  - Command Line
  - SAP services/tools
- Auditing and Compliance
- **OS and Network Security**
- References and Important OSS notes

# OS and Network Security

- OS and network security is as important as database and application security
- OS Security patches should be installed regularly
- Minimal OS package installation for fewer security holes. The added benefit is that you need to install fewer OS patches.
- OS user password policy
- Cron and at permissions (disable at jobs for all)
- File permissions and umask
- Logging and forwarding
- No ssh login allowed for root account (/etc/ssh/sshd.conf – PermitRootLogin no)
- Install security checker
- Restrict sudo for normal user
- Do not allow sudo for vi
  - [admin@sapecc ~]\$ sudo vi x
  - exit from vi
  - [root@sapecc ~]# id
  - uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),5011(sapinst)
- Consider deploying HANA firewall

# SUSE Linux Security

<https://www.suse.com/support/security/>

Customer Center Contact Account English Search Let's Chat

Products & Solutions Support & Services Partners Communities About Free Downloads Shop

Support SUSE Security

Read the news on sale of SUSE to EQT >

## SUSE Security

# A Process That Never Ends

**SUSE is committed to delivering best effort security to its customers and to the Open Source community. We believe that trust in Open Source Software security in general, and the user privacy in particular, are both indispensable and infeasible.**

Let's Chat

# SUSE Security Patch Day

<https://wiki.scn.sap.com/wiki/display/PSR/The+Official+SAP+Product+Security+Response+Space>

The screenshot shows a web browser window displaying the SAP Community Wiki page titled "The Official SAP Product Security Response Space". The browser's address bar shows the URL: <https://wiki.scn.sap.com/wiki/display/PSR/The+Official+SAP+Product+Security+Response+Space>. The page header includes the SAP logo, "Community WIKI", "SAP Community", and navigation links for "Welcome, Guest", "Login", and "Register". A search bar is present with the text "Search the Community". Below the header, there are navigation options for "Spaces", "Browse", and "Create". The main content area features the title "The Official SAP Product Security Response Space" and a sub-header "Product Security Response at SAP". It states that the page was created by Aditi Kulkarni and last modified on Mar 12, 2019. The main text describes SAP's commitment to security, mentioning its global leadership, collaboration with external researchers, and the implementation of a well-defined Security Response Process. Below the main text, there are two columns of links: "Recent Blog Posts" and "Links".

**Recent Blog Posts**

- [SAP Security Patch Day - March 2019](#)
- [SAP Security Patch Day - February 2019](#)
- [SAP Security Patch Day - January 2019](#)

› Blogs from 2018  
› Blogs from 2017  
› Blogs from 2016  
› Blogs from 2015

**Links:**

- [Acknowledgements to Security Researchers](#)
- [Report a Security Issue to SAP](#)
- [Report a Customer Incident](#)
- [SAP Security Notes](#)
- [SAP Patch Day FAQ](#)
- [Introduction to CVSS. How SAP uses it?](#)
- [SAP Disclosure Guidelines](#)

# Agenda

- Fitch Overview
- Traditional vs. HANA Database Security
- Security Administration
  - User and group administration
  - Privileges and Roles
- Tools –
  - HANA Studio,
  - HANA Cockpit
  - Web-based Development workbench
  - Command Line
  - SAP services/tools
- Auditing and Compliance
- OS and Network Security
- References and Important OSS notes



# References

- SAP HANA Security Guide
  - [https://help.sap.com/doc/eec734dbb0fd1014a61590fcb5411390/2.0.03/en-US/SAP\\_HANA\\_Security\\_Guide\\_en.pdf](https://help.sap.com/doc/eec734dbb0fd1014a61590fcb5411390/2.0.03/en-US/SAP_HANA_Security_Guide_en.pdf)
- SAP HANA Administration Guide
  - [https://help.sap.com/doc/eb75509ab0fd1014a2c6ba9b6d252832/2.0.03/en-US/SAP\\_HANA\\_Administration\\_Guide\\_en.pdf](https://help.sap.com/doc/eb75509ab0fd1014a2c6ba9b6d252832/2.0.03/en-US/SAP_HANA_Administration_Guide_en.pdf)
- SAP HANA Security Checklists and Recommendations
  - [https://help.sap.com/doc/3cffa43c8e3843cdae23f9abfe47355e/2.0.03/en-US/SAP\\_HANA\\_Security\\_Checklists\\_and\\_Recommendations\\_en.pdf](https://help.sap.com/doc/3cffa43c8e3843cdae23f9abfe47355e/2.0.03/en-US/SAP_HANA_Security_Checklists_and_Recommendations_en.pdf)
- ASUG Presentations
- SAP TechEd Presentations
- SAP Security Patch day <https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html>
- SAP HANA Academy on YouTube
- SAP blogs
- Comparing XS Classic to XS Advanced
  - <https://help.sap.com/viewer/58d81eb4c9bc4899ba972c9fe7a1a115/2.0.00/en-US/b1333dbbfa9549ffa76850b5b5ca455a.html>
- SUSE Linux Security - <https://www.suse.com/support/security>
- SAP HANA Security - An Overview - <https://archive.sap.com/documents/docs/DOC-62943>

# Important OSS notes

- 2159014 - FAQ: SAP HANA Security
- 2535951 - FAQ: SAP HANA Users and Schemas
- 2477204 - FAQ: SAP HANA Services and Ports
- 2378962 - SAP HANA 2.0 Revision and Maintenance Strategy
- 1837331 – HOW TO HANA DB SSO Kerberos/ Active Directory ( Kerberos Guide attached)
- 1731000 - Configuration changes that are not recommended ( No SELinux )
- 2093286 - Migration from OpenSSL to CommonCryptoLib
- 1718944 - SAP HANA DB: Securing External SQL Communication (CommonCryptoLib)
- 2175672 - Migration steps from manual SSL configuration for internal communication to automatic configuration using system PKI
- 2097613 - Database is running with inconsistent Secure Storage File System (SSFS)
- 2183624 - Potential information leakage using default SSFS master key in HANA
- 863362 - Security checks in SAP EarlyWatch Alert, EarlyWatch and GoingLive sessions
- 2228829 - How to Change the DPAPI Root Key
- 2380291 - SAP HANA 2.0 Cockpit Central Release Note

# Take the Session Survey.

We want to hear from you! Be sure to complete the session evaluation on the SAPPHIRE NOW and ASUG Annual Conference mobile app.



# Presentation Materials

Access the slides from 2019 ASUG Annual Conference here:

<http://info.asug.com/2019-ac-slides>

# Q&A

For questions after this session, contact us at [ranjit.prithviraj@fitchratings.com](mailto:ranjit.prithviraj@fitchratings.com)  
and [sanjay.mahajan@fitchratings.com](mailto:sanjay.mahajan@fitchratings.com).

# Let's Be Social.

Stay connected. Share your SAP experiences anytime, anywhere.

Join the ASUG conversation on social media: **@ASUG365 #ASUG**

