asug
Americas' SAP Users' Group

Nexperia designs State-of-the-art Security with BW on HANA

Tim Lynen, Director, axl & trax
Raymond De Ruiter, Senior Busines Process Expert, Nexperia

Session ID #83780

SAP SAPPHIRENOW | asug ANNUAL CONFERENCE

May 7 – 9, 2019

About the Speakers

Tim Lynen

- Director, axl & trax NV
- +15 years experience in different SAP security technologies (ABAP, HANA, Java)
- CRISC & SAP security certified

Raymond De Ruiter

- Sr, BPE Security, Nexperia
- +15 years experience in SAP security (ABAP, HANA) & SAP Fraude Mgt.
- SAP BW developer
- I wish I became a football player

Key Outcomes/Objectives

1. understand the security model/concept in a HANA database
2. Implement a role based access model in security segregating business & IT responsibilities
3. understand & implement detective controls

Agenda

- Overview of the project scope
- Quick SAP HANA security overview
- Implementation of HANA authorizations
- (Security) audit log
- Native HANA transport landscape

Overview of the project scope

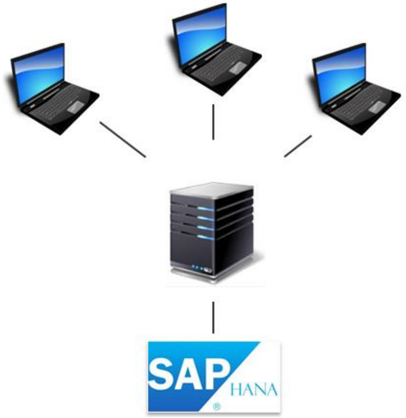
- System in scope
  - SAP BW (7.40) on HANA system

- Project scope
  - harden HANA default security settings
  - implement a state-of-the-art access model for business users
  - establish detective monitoring and audit capabilities
  - enforce adequate change management

HANA security model scenario’s

Nexperia situation

REGULAR

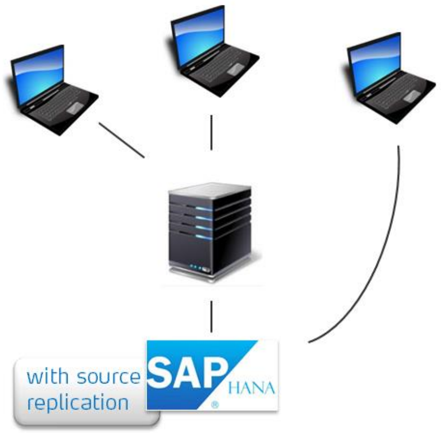


Traditional

- DB migration to HANA

➢ No changes to security model

HYBRID

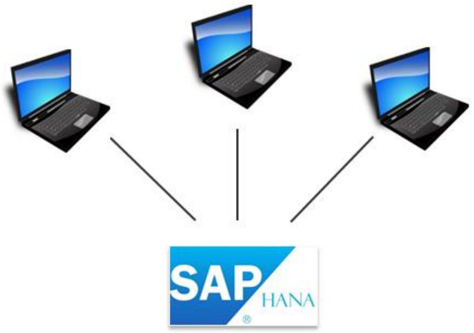


Data mart (3-tier or 2-tier)

- Reporting ERP or BW data in HANA
- Direct user access to HANA

➢ **Modified** security model

NATIVE



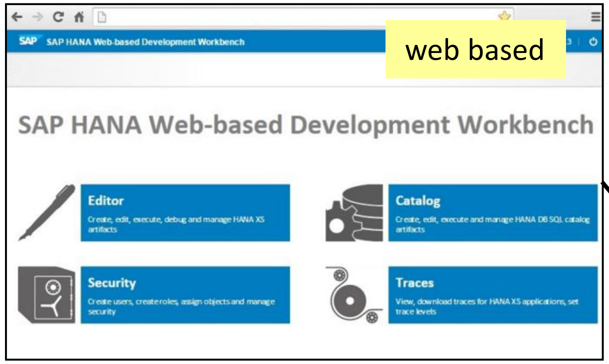
Native 2-tier application

- HANA acts as DB & Application Server
- Direct user access to HANA

➢ **Integrated** security model

Difference between design time and run time

SAP HANA Web **I**nteractive **D**eveloping **E**nvironment



web based

SAP HANA Web-based Development Workbench

SAP HANA Web-based Development Workbench

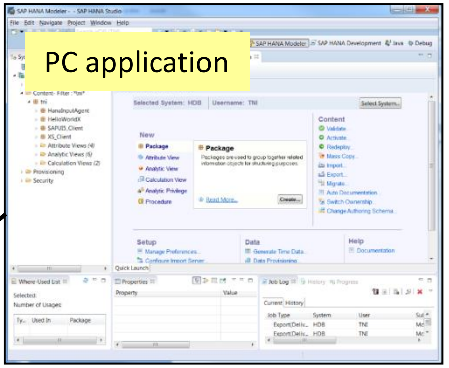
Editor
Create, edit, execute, debug and manage HANA XS artifacts

Catalog
Create, edit, execute and manage HANA DB SQL catalog artifacts

Security
Create users, create roles, assign objects and manage security

Traces
View, download traces for HANA XS applications, set trace levels

SAP HANA Studio



PC application

both tools for both design time and run time, but SAP HANA Studio is more technical and will be decommissioned in time.

SAP HANA System

DESIGN TIME

This is where developers develop most of the building blocks of SAP HANA.

All these development objects are owned by the system user _SYS_REPO

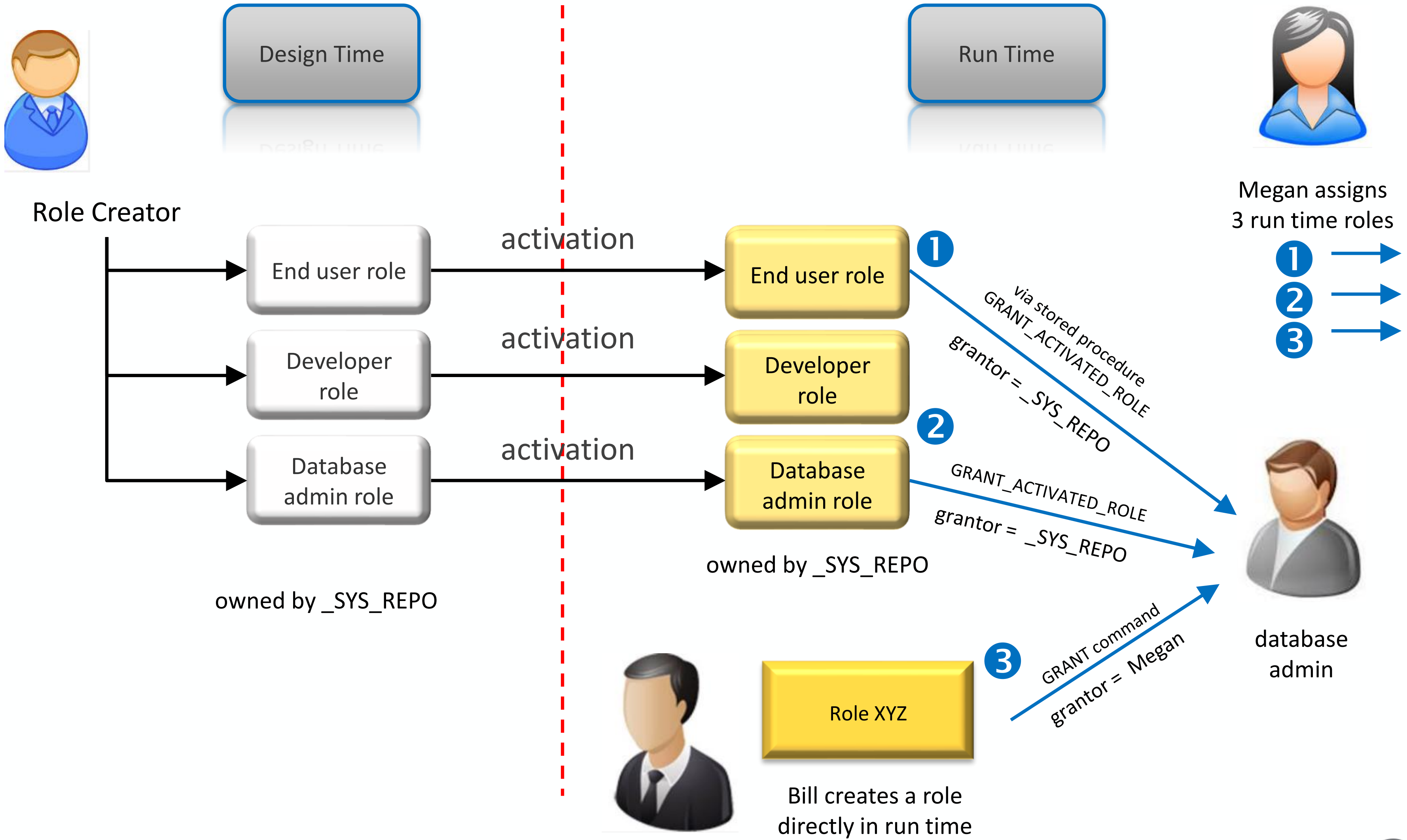
RUN TIME

SAP HANA building blocks can equally be created and maintained in run time, which means they are translated into SQL code in the background and applied directly to the HANA database.

All these run time objects are owned by the database user who created them.

If the creator is removed from the HANA DB, then the owned runtime objects are removed too.

Role building in HANA



Authorizations in HANA – Privilege types

Design Time

Content

Package

<my company>

own security roles

System priv

- Comparable with S_ADMI_FCD object
- For HANA database related tasks such as catalog and schema mngt, auditing, system mngt, data import and export, users and roles mngt

Application priv

- For example web interface for user/role maintenance

Package priv

- Only for developers, modelers (incl. role admin)
- READ, EDIT, ACTIVATE, MAINTAIN (create sub package in (sub)package

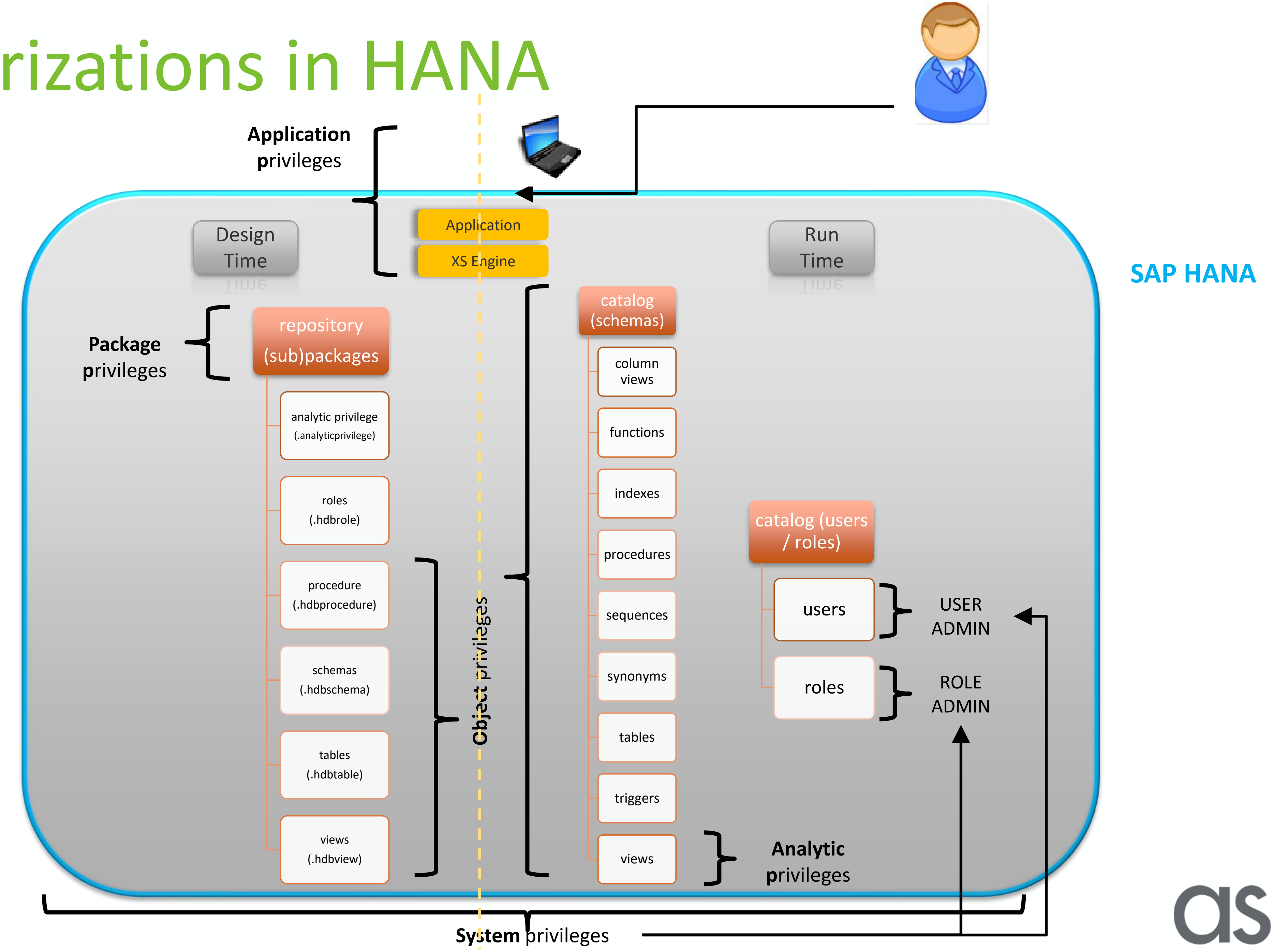
Object priv

- Access to database objects like schemas, tables, views, function/procedures, sequences, remote source, personal security environment
- Essential to do anything in HANA

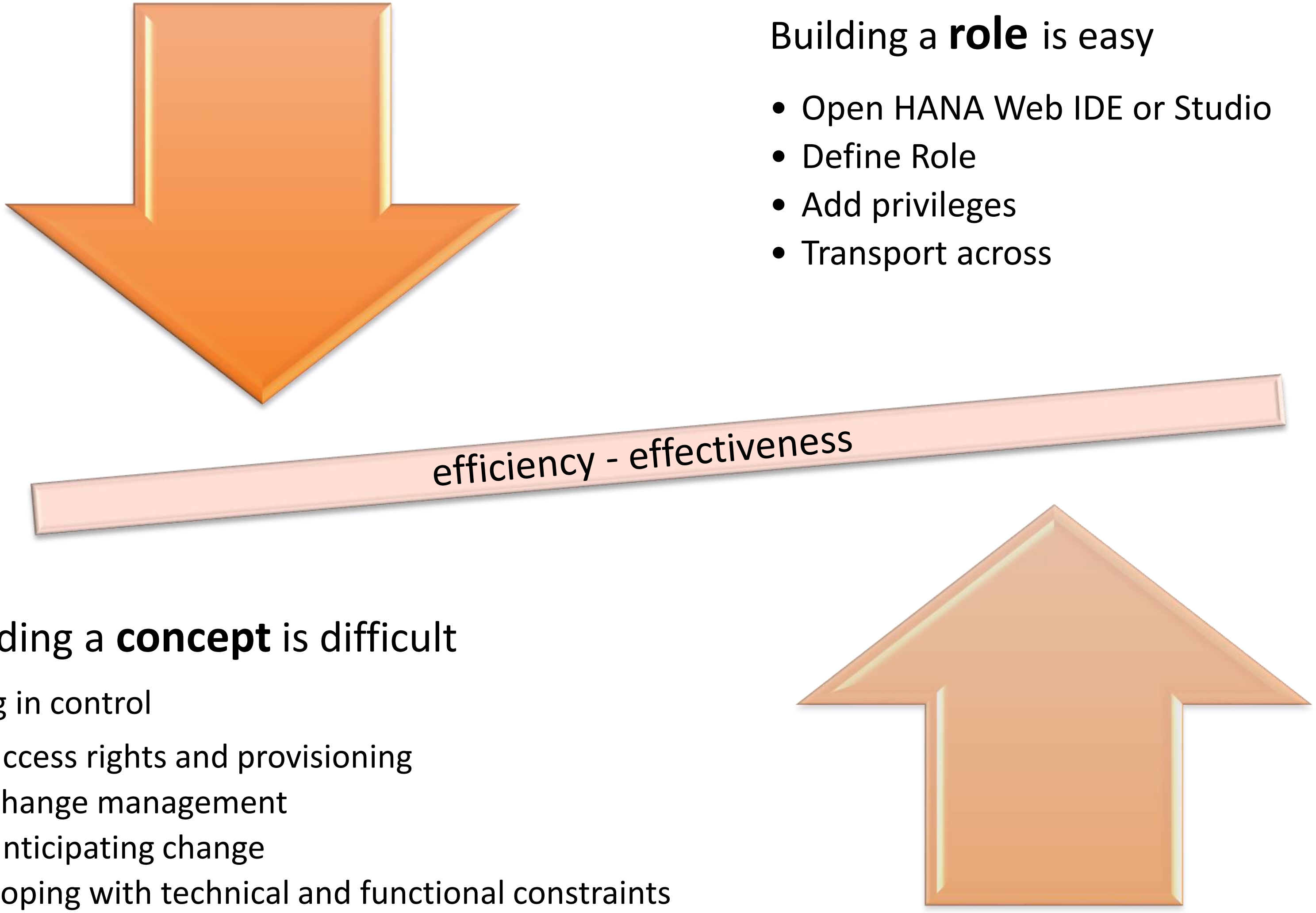
Analytic priv

- For row level restrictions on table content
- Restrictions should be built as repository objects before they can be assigned to a role
- static (fixed restricted values) or dynamic (lookup in tables with matching fields ; e.g.. cost center limitation per user)

Authorizations in HANA



HANA authorization concept considerations



Building a **role** is easy

- Open HANA Web IDE or Studio
- Define Role
- Add privileges
- Transport across

efficiency - effectiveness

Building a **concept** is difficult

Being in control

- of access rights and provisioning
- of change management
- of anticipating change
- of coping with technical and functional constraints

Role Based Access Control

- A layered authorization concept splitting technical authorizations from business functions and user management
  - Building blocks (Lego blocks)
  - Functions (business functions)
  - Users (actual end users)
- Segregation between responsibilities of IT & business
- Structured way of working
  - Avoid having multiple privileges in multiple building blocks
  - Templatize privilege management for better control and transparency

Role mngt – package structure – building blocks

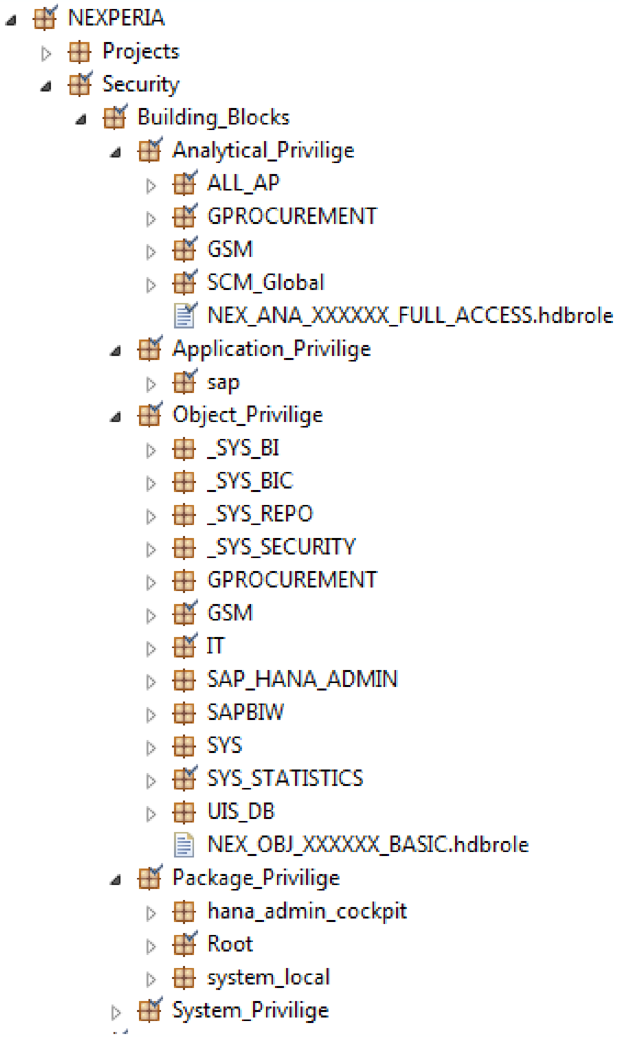
Design Time

Content

Package

<my company>

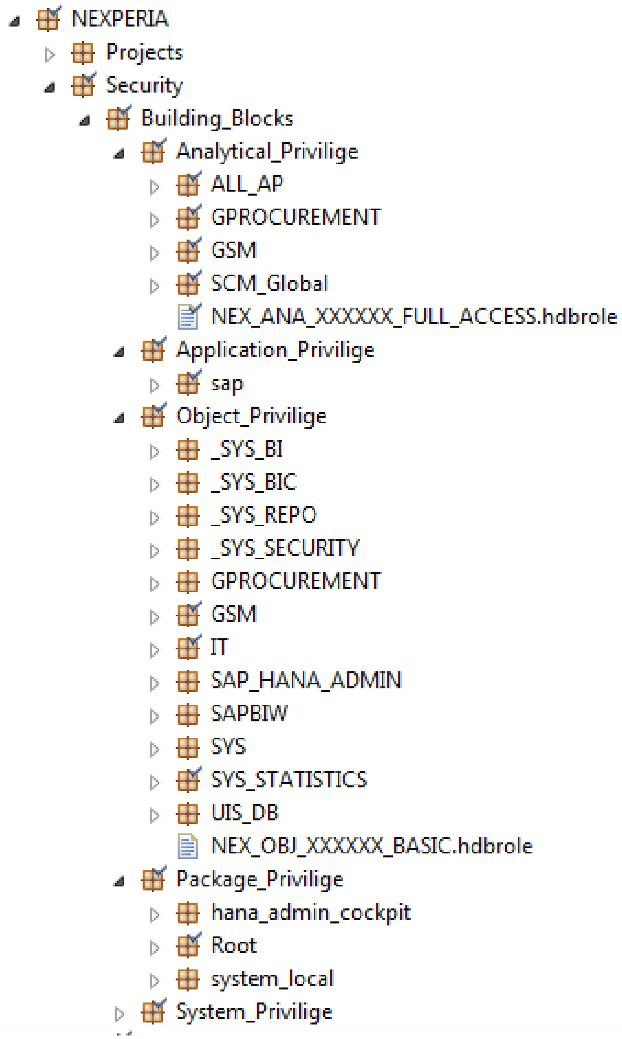
own security roles



- NEXPERIA
  - Projects
  - Security
    - Building_Blocks
      - Analytical_Privilige
        - ALL_AP
        - GPROCUREMENT
        - GSM
        - SCM_Global
        - NEX_ANA_XXXXXX_FULL_ACCESS.hdbrole
      - Application_Privilige
        - sap
      - Object_Privilige
        - _SYS_BI
        - _SYS_BIC
        - _SYS_REPO
        - _SYS_SECURITY
        - GPROCUREMENT
        - GSM
        - IT
        - SAP_HANA_ADMIN
        - SAPBIW
        - SYS
        - SYS_STATISTICS
        - UIS_DB
        - NEX_OBJ_XXXXXX_BASIC.hdbrole
      - Package_Privilige
        - hana_admin_cockpit
        - Root
        - system_local
      - System_Privilige

- Privileges are structured per type of privilege
  - Analytic
  - Application
  - Object
  - Package
  - System

Role naming convention



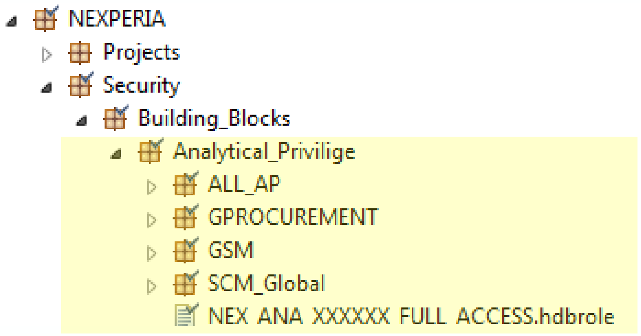
- NEXPERIA
  - Projects
  - Security
    - Building_Blocks
      - Analytical_Privilige
        - ALL_AP
        - GPROCUREMENT
        - GSM
        - SCM_Global
        - NEX_ANA_XXXXXX_FULL_ACCESS.hdbrole
      - Application_Privilige
        - sap
      - Object_Privilige
        - _SYS_BI
        - _SYS_BIC
        - _SYS_REPO
        - _SYS_SECURITY
        - GPROCUREMENT
        - GSM
        - IT
        - SAP_HANA_ADMIN
        - SAPBIW
        - SYS
        - SYS_STATISTICS
        - UIS_DB
        - NEX_OBJ_XXXXXX_BASIC.hdbrole
      - Package_Privilige
        - hana_admin_cockpit
        - Root
        - system_local
      - System_Privilige

- Role naming and package structure go hand in hand

- Design-time = tree structure

- Run-time = flat view separated by dots
  - **e.g,** NEXPERIA.Security.Building_Blocks.Analytical_privileges.*NEX_ANA_XXXXX_FULL_ACCESS.hdbrole*

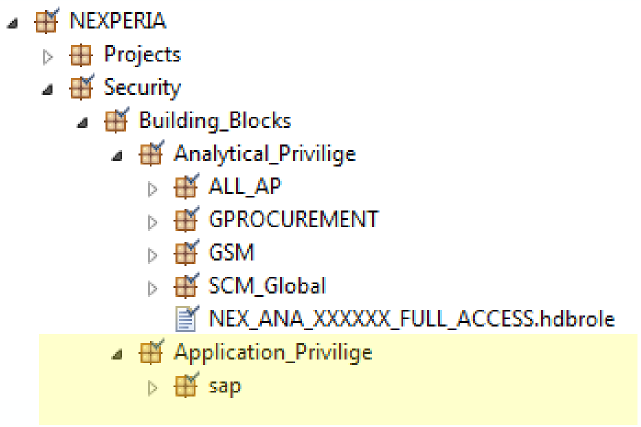
Analytic privileges



```
NEXPERIA
  Projects
  Security
    Building_Blocks
      Analytical_Privilige
        ALL_AP
        GPROCUREMENT
        GSM
        SCM_Global
        NEX ANA XXXXXX FULL ACCESS.hdbrole
```

- Used to secure data on line item level
- Have to be built in / created by the creator of the data views
- Structured per line of business

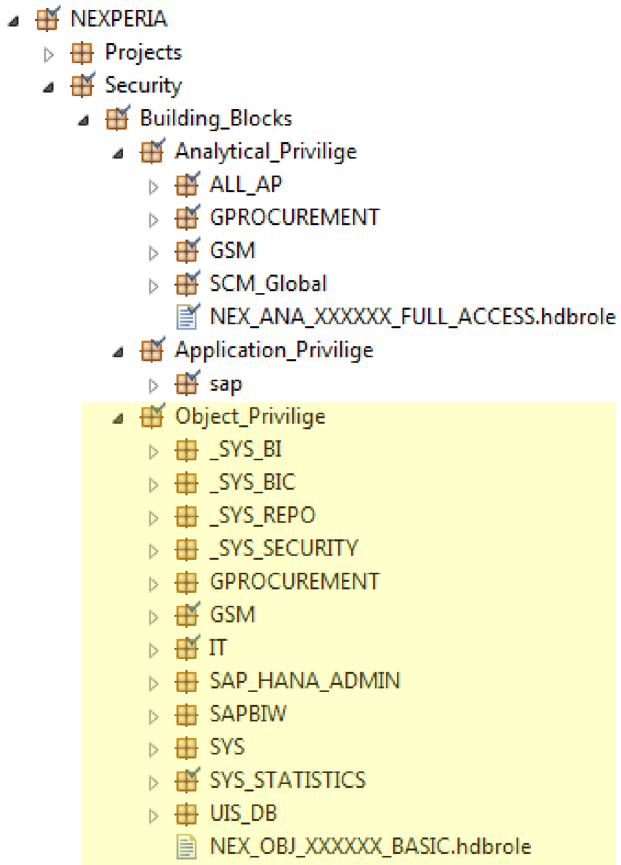
Application privileges



- NEXPERIA
  - Projects
  - Security
    - Building_Blocks
      - Analytical_Privilige
        - ALL_AP
        - GPROCUREMENT
        - GSM
        - SCM_Global
        - NEX_ANA_XXXXXX_FULL_ACCESS.hdbrole
      - Application_Privilige
        - sap

- Needed to use HANA native XS applications
  - Delivered by SAP
    - Like the web interface for user/role management
  - Created in house/3rd party
    - Own created XS applications

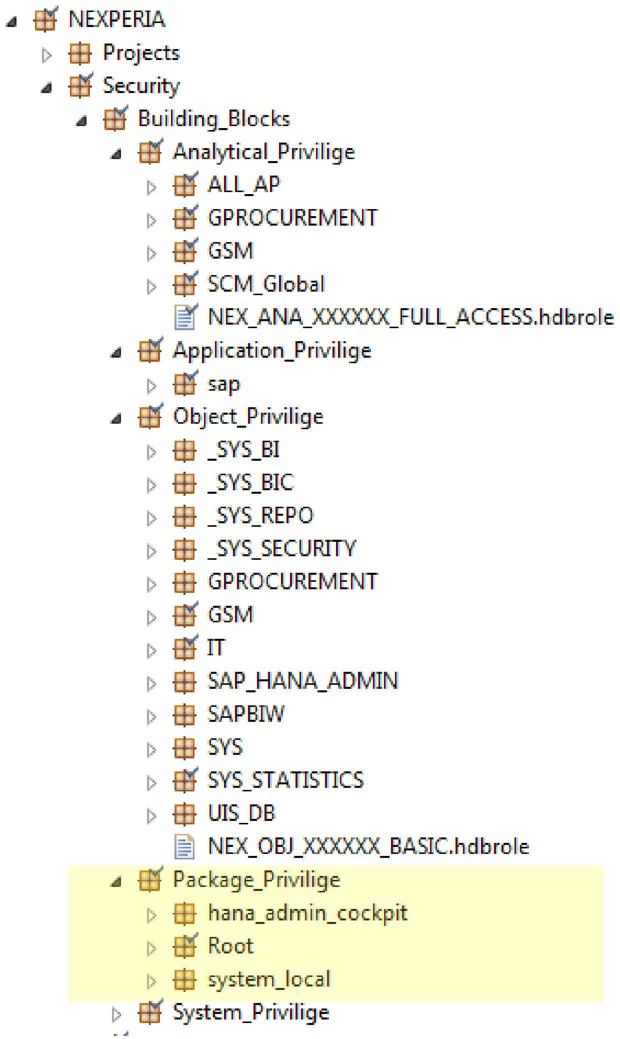
Object privileges



- NEXPERIA
  - Projects
  - Security
    - Building_Blocks
      - Analytical_Privilige
        - ALL_AP
        - GPROCUREMENT
        - GSM
        - SCM_Global
        - NEX_ANA_XXXXXX_FULL_ACCESS.hdbrole
      - Application_Privilige
        - sap
      - Object_Privilige
        - _SYS_BI
        - _SYS_BIC
        - _SYS_REPO
        - _SYS_SECURITY
        - GPROCUREMENT
        - GSM
        - IT
        - SAP_HANA_ADMIN
        - SAPBIW
        - SYS
        - SYS_STATISTICS
        - UIS_DB
        - NEX_OBJ_XXXXXX_BASIC.hdbrole

- Needed for data access
- Structured by database schema
- Basic role that will be granted to all functions
- Possibility to segregate between display & maintenance access
  - SELECT vs UPDATE/CREATE/DELETE

Package privileges



- NEXPERIA
  - Projects
  - Security
    - Building_Blocks
      - Analytical_Privilige
        - ALL_AP
        - GPROCUREMENT
        - GSM
        - SCM_Global
        - NEX_ANA_XXXXXX_FULL_ACCESS.hdbrole
      - Application_Privilige
        - sap
      - Object_Privilige
        - _SYS_BI
        - _SYS_BIC
        - _SYS_REPO
        - _SYS_SECURITY
        - GPROCUREMENT
        - GSM
        - IT
        - SAP_HANA_ADMIN
        - SAPBIW
        - SYS
        - SYS_STATISTICS
        - UIS_DB
        - NEX_OBJ_XXXXXX_BASIC.hdbrole
      - Package_Privilige
        - hana_admin_cockpit
        - Root
        - system_local
      - System_Privilige

- Needed in design time only
- Not needed for end users
- To structure the way of working and segregate between projects, security, …
- Best practices exist for setting up a package structure

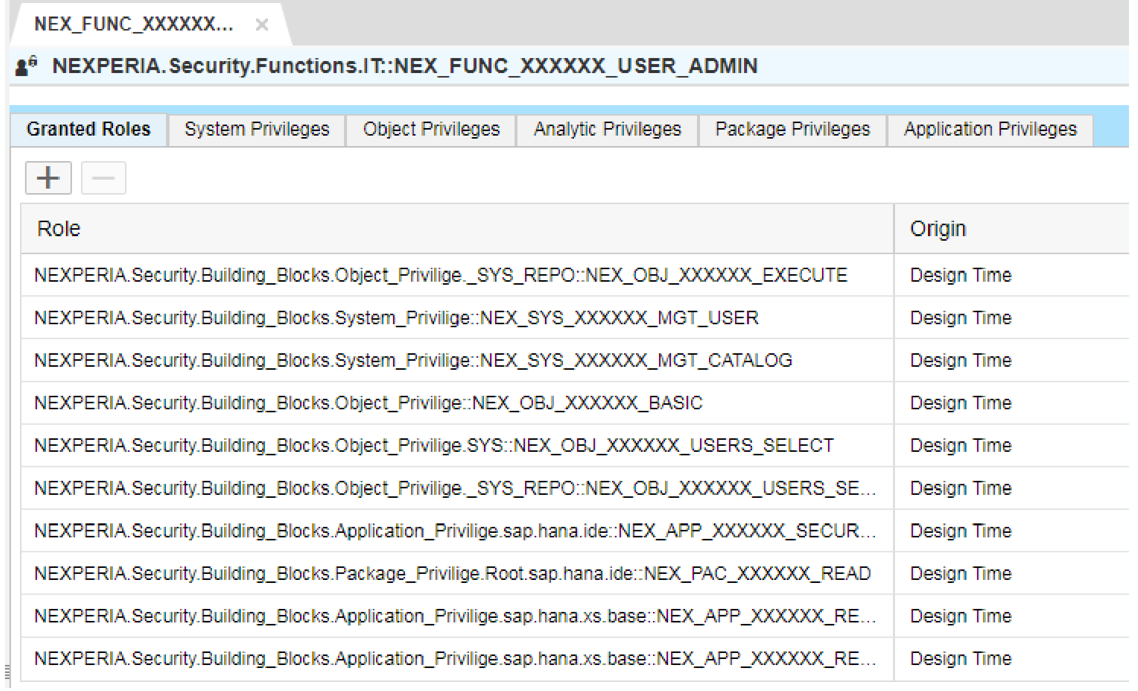
System privileges

- Only a limited number of system privileges exist (46 in v2.0.2)
- Not needed for end users
- Only needed for specific system related tasks
- Can be clustered by task (backup, security, audit, performance & settings, …)

source: https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.02/en-US/2a942546f16846d597177b3bfbd1df04.html

Business function design

- Functions tailored to functions in the business & IT department
    - Ex. User Administrator
- Structured per department
    - IT, HR, Finance, Sales, …
- Functions only contain building blocks, no direct privileges to respect the RBAC model
- Users only get functions assigned

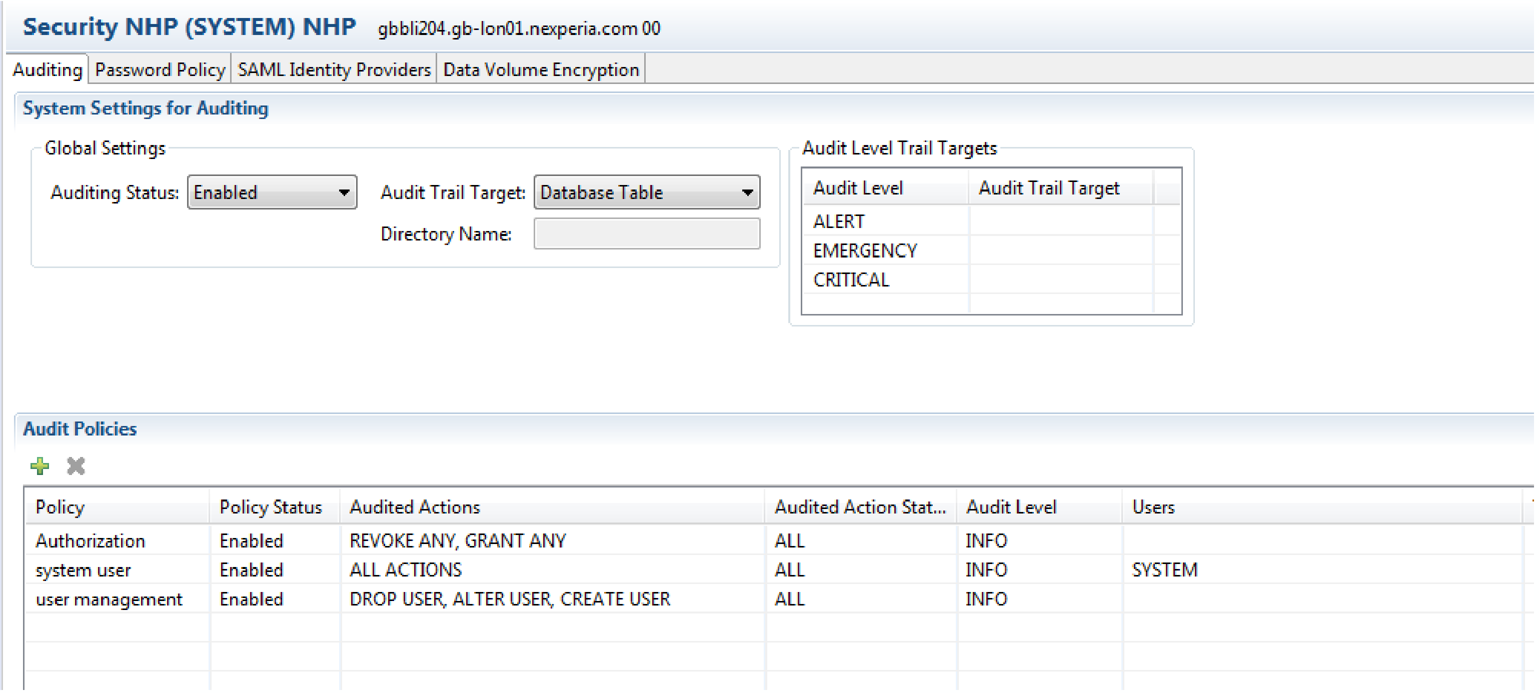


NEXPERIA.Security.Functions.IT::NEX_FUNC_XXXXXX_USER_ADMIN

Role	Origin
NEXPERIA.Security.Building_Blocks.Object_Privilige._SYS_REPO::NEX_OBJ_XXXXXX_EXECUTE	Design Time
NEXPERIA.Security.Building_Blocks.System_Privilige::NEX_SYS_XXXXXX_MGT_USER	Design Time
NEXPERIA.Security.Building_Blocks.System_Privilige::NEX_SYS_XXXXXX_MGT_CATALOG	Design Time
NEXPERIA.Security.Building_Blocks.Object_Privilige::NEX_OBJ_XXXXXX_BASIC	Design Time
NEXPERIA.Security.Building_Blocks.Object_Privilige.SYS::NEX_OBJ_XXXXXX_USERS_SELECT	Design Time
NEXPERIA.Security.Building_Blocks.Object_Privilige._SYS_REPO::NEX_OBJ_XXXXXX_USERS_SE...	Design Time
NEXPERIA.Security.Building_Blocks.Application_Privilige.sap.hana.ide::NEX_APP_XXXXXX_SECUR...	Design Time
NEXPERIA.Security.Building_Blocks.Package_Privilige.Root.sap.hana.ide::NEX_PAC_XXXXXX_READ	Design Time
NEXPERIA.Security.Building_Blocks.Application_Privilige.sap.hana.xs.base::NEX_APP_XXXXXX_RE...	Design Time
NEXPERIA.Security.Building_Blocks.Application_Privilige.sap.hana.xs.base::NEX_APP_XXXXXX_RE...	Design Time

Security audit log - setup

- What’s logged
  - All SYSTEM user activities
  - All user & role management activities
- Best practices from SAP available https://archive.sap.com/documents/docs/DOC-51098



Security NHP (SYSTEM) NHP gbbli204.gb-lon01.nexperia.com 00

System Settings for Auditing

Global Settings

Auditing Status: Enabled

Audit Trail Target: Database Table

Directory Name:

Audit Level Trail Targets

Audit Level	Audit Trail Target
ALERT	
EMERGENCY	
CRITICAL	

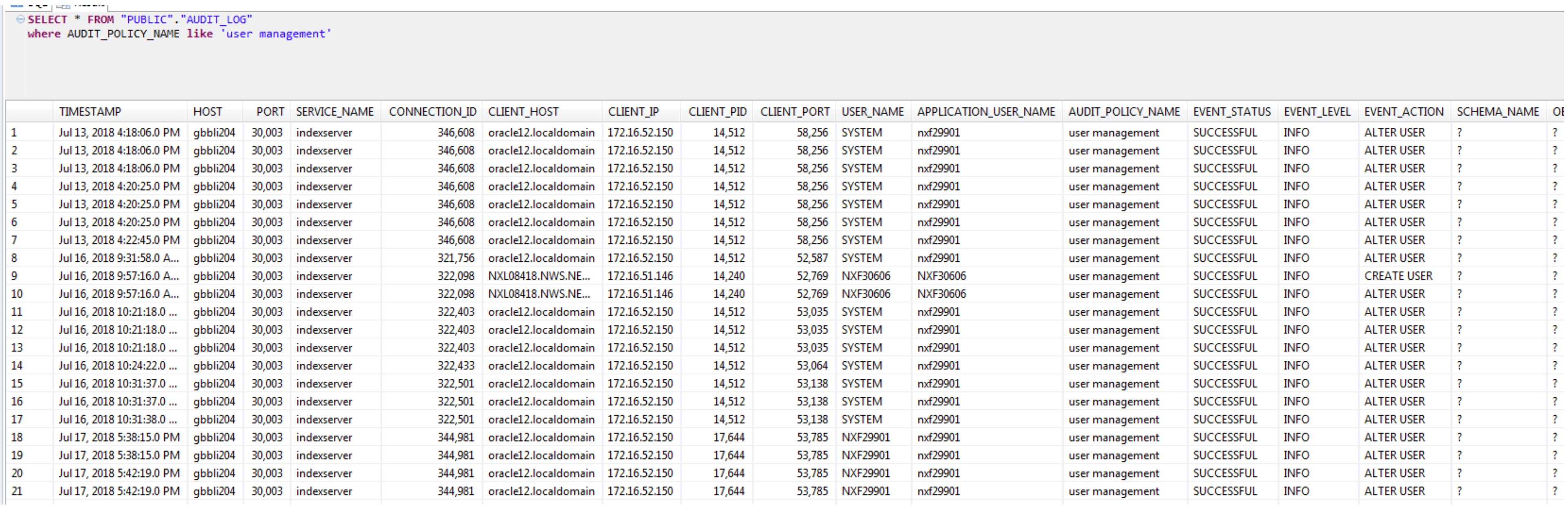
Audit Policies

Policy	Policy Status	Audited Actions	Audited Action Stat...	Audit Level	Users
Authorization	Enabled	REVOKE ANY, GRANT ANY	ALL	INFO	
system user	Enabled	ALL ACTIONS	ALL	INFO	SYSTEM
user management	Enabled	DROP USER, ALTER USER, CREATE USER	ALL	INFO	

Security audit log – read log data

- Table with results is available in PUBLIC namespace (to be considered in role & authorization design – not everyone needs/should have access)

- SELECT all OR by defined policy possible (views can be created as certain people only need certain data to be visible)

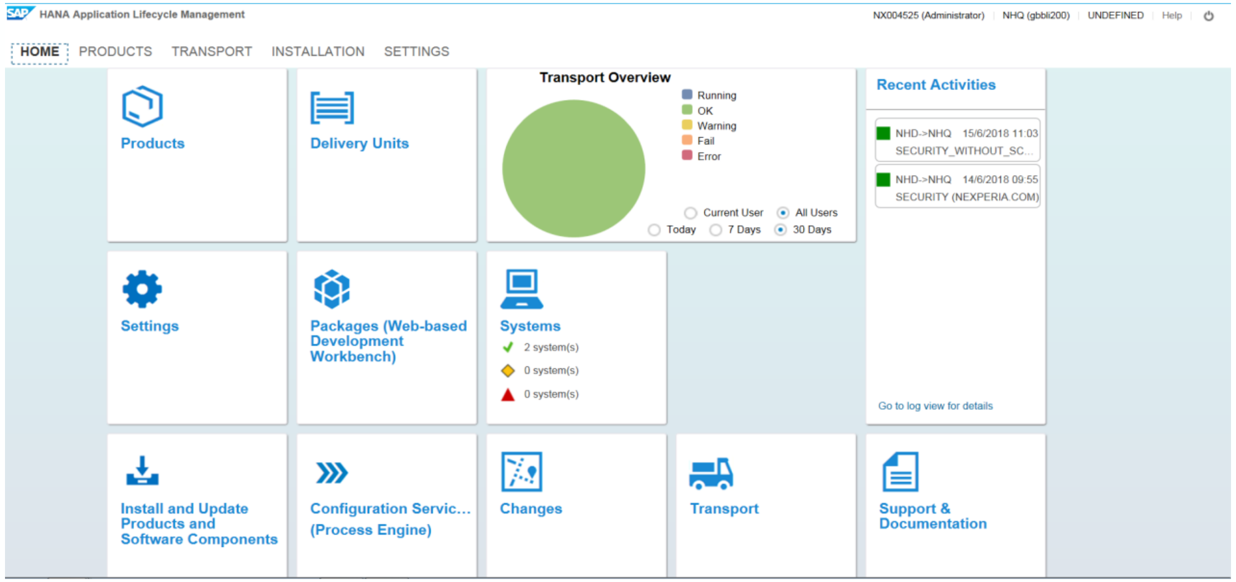


```
SELECT * FROM "PUBLIC"."AUDIT_LOG"
where AUDIT_POLICY_NAME like 'user management'
```

	TIMESTAMP	HOST	PORT	SERVICE_NAME	CONNECTION_ID	CLIENT_HOST	CLIENT_IP	CLIENT_PID	CLIENT_PORT	USER_NAME	APPLICATION_USER_NAME	AUDIT_POLICY_NAME	EVENT_STATUS	EVENT_LEVEL	EVENT_ACTION	SCHEMA_NAME	OI
1	Jul 13, 2018 4:18:06.0 PM	gbbli204	30,003	indexserver	346,608	oracle12.localdomain	172.16.52.150	14,512	58,256	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
2	Jul 13, 2018 4:18:06.0 PM	gbbli204	30,003	indexserver	346,608	oracle12.localdomain	172.16.52.150	14,512	58,256	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
3	Jul 13, 2018 4:18:06.0 PM	gbbli204	30,003	indexserver	346,608	oracle12.localdomain	172.16.52.150	14,512	58,256	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
4	Jul 13, 2018 4:20:25.0 PM	gbbli204	30,003	indexserver	346,608	oracle12.localdomain	172.16.52.150	14,512	58,256	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
5	Jul 13, 2018 4:20:25.0 PM	gbbli204	30,003	indexserver	346,608	oracle12.localdomain	172.16.52.150	14,512	58,256	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
6	Jul 13, 2018 4:20:25.0 PM	gbbli204	30,003	indexserver	346,608	oracle12.localdomain	172.16.52.150	14,512	58,256	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
7	Jul 13, 2018 4:22:45.0 PM	gbbli204	30,003	indexserver	346,608	oracle12.localdomain	172.16.52.150	14,512	58,256	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
8	Jul 16, 2018 9:31:58.0 A...	gbbli204	30,003	indexserver	321,756	oracle12.localdomain	172.16.52.150	14,512	52,587	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
9	Jul 16, 2018 9:57:16.0 A...	gbbli204	30,003	indexserver	322,098	NXL08418.NWS.NE...	172.16.51.146	14,240	52,769	NXF30606	NXF30606	user management	SUCCESSFUL	INFO	CREATE USER	?	?
10	Jul 16, 2018 9:57:16.0 A...	gbbli204	30,003	indexserver	322,098	NXL08418.NWS.NE...	172.16.51.146	14,240	52,769	NXF30606	NXF30606	user management	SUCCESSFUL	INFO	ALTER USER	?	?
11	Jul 16, 2018 10:21:18.0 ...	gbbli204	30,003	indexserver	322,403	oracle12.localdomain	172.16.52.150	14,512	53,035	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
12	Jul 16, 2018 10:21:18.0 ...	gbbli204	30,003	indexserver	322,403	oracle12.localdomain	172.16.52.150	14,512	53,035	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
13	Jul 16, 2018 10:21:18.0 ...	gbbli204	30,003	indexserver	322,403	oracle12.localdomain	172.16.52.150	14,512	53,035	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
14	Jul 16, 2018 10:24:22.0 ...	gbbli204	30,003	indexserver	322,433	oracle12.localdomain	172.16.52.150	14,512	53,064	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
15	Jul 16, 2018 10:31:37.0 ...	gbbli204	30,003	indexserver	322,501	oracle12.localdomain	172.16.52.150	14,512	53,138	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
16	Jul 16, 2018 10:31:37.0 ...	gbbli204	30,003	indexserver	322,501	oracle12.localdomain	172.16.52.150	14,512	53,138	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
17	Jul 16, 2018 10:31:38.0 ...	gbbli204	30,003	indexserver	322,501	oracle12.localdomain	172.16.52.150	14,512	53,138	SYSTEM	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
18	Jul 17, 2018 5:38:15.0 PM	gbbli204	30,003	indexserver	344,981	oracle12.localdomain	172.16.52.150	17,644	53,785	NXF29901	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
19	Jul 17, 2018 5:38:15.0 PM	gbbli204	30,003	indexserver	344,981	oracle12.localdomain	172.16.52.150	17,644	53,785	NXF29901	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
20	Jul 17, 2018 5:42:19.0 PM	gbbli204	30,003	indexserver	344,981	oracle12.localdomain	172.16.52.150	17,644	53,785	NXF29901	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?
21	Jul 17, 2018 5:42:19.0 PM	gbbli204	30,003	indexserver	344,981	oracle12.localdomain	172.16.52.150	17,644	53,785	NXF29901	nxf29901	user management	SUCCESSFUL	INFO	ALTER USER	?	?

SAP HANA Native transport mechanism

- Available via a native SAP HANA XS application
- Items that need configuration
  - Systems need to be set up
  - Transport routes need to be created
- Items that need to be done by modelers/developers
  - Packages need to be attached to delivery units


HANA Application Lifecycle Management
NX004525 (Administrator) | NHQ (gbbli200) | UNDEFINED | Help
HOME
PRODUCTS
TRANSPORT
INSTALLATION
SETTINGS
Products
Delivery Units
Transport Overview
Running
OK
Warning
Fail
Error
Recent Activities
Settings
Packages (Web-based Development Workbench)
Systems
Install and Update Products and Software Components
Configuration Servic... (Process Engine)
Changes
Transport
Support & Documentation

○ Current User ● All Users
○ Today ○ 7 Days ● 30 Days

NHD->NHQ 15/6/2018 11:03 SECURITY_WITHOUT_SC...

NHD->NHQ 14/6/2018 09:55 SECURITY (NEXPERIA.COM)

Go to log view for details

✓ 2 system(s)
◆ 0 system(s)
▲ 0 system(s)

Lessons learned

- KISS – Keep It Simple, Stupid
- Design time is the place to be
- Web interface is much easier / user friendly
- Work together with development for the application & analytic privilege setup
- Transporting is easy if you defined your roles correct

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.

ASUG

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 tim.lynen@axl-trax.com and raymond.de.ruiter@nexperia.com

Let’s Be Social.

Stay connected. Share your SAP experiences anytime, anywhere.

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