# Kapitel 4 Sicherheit in Multi-Tenant-Datenbanken

In diesem Kapitel erfahren Sie, welche Sicherheitsanforderungen für Multi-Tenant-Systeme bestehen und wie sie im System umgesetzt werden können.

Die Sicherheit einer SAP-HANA-Datenbank teilt sich in mehrere Bereiche auf. Die Datenbankadministratoren sind maßgeblich in der Systemdatenbank tätig. Dort befinden sich keine betriebswirtschaftlichen Daten. Diese werden in den Tenants gespeichert und verwaltet. Jede SAP-HANA-Datenbank besteht aus einer Systemdatenbank und mindestens einem Tenant. Die Tenants sind so gekapselt, dass tenantübergreifende Zugriffe standardmäßig nicht möglich sind. Ein lesender Zugriff kann allerdings tenant-übergreifend eingerichtet werden.

In Abschnitt 4.1, »Das Konzept der Tenant-Datenbanken«, erkläre ich Ihnen das Konzept und den grundlegenden Aufbau von Multi-Tenant-Datenbanken. Mit den tenant-übergreifenden Zugriffen befasse ich mich im gleichnamigen Abschnitt 4.2. Welche Möglichkeiten es gibt, um Tenants abzusichern und zu kapseln, erfahren Sie in Abschnitt 4.3, »Nicht änderbare Parameter in Tenants«, bis Abschnitt 4.5, »High Isolation Level für Tenants«. Abschließend finden Sie in Abschnitt 4.6, »Protokollierung von Änderungen an Tenants«, die Einstellungen zur Protokollierung von Änderungen an Tenants.

## 4.1 Das Konzept der Tenant-Datenbanken

Bis zu SAP HANA Release 2.0 SPSO gab es zwei mögliche Installationen einer SAP-HANA-Datenbank:

#### Single-Container-Systeme

Single-Container-Systeme sind Datenbanken mit nur einem Container, in dem alle Benutzer eingerichtet sind, in dem die produktiven Daten liegen und in dem die Entwicklung stattfindet.

#### Multi-Tenant-Systeme

Multi-Tenant-Systeme sind Datenbanken mit einer Systemdatenbank und 1-n *Tenant-Datenbanken*. Die Verwaltung der Datenbank selbst erfolgt über die System-DB. Die betriebswirtschaftlichen Daten werden in den Tenants verwaltet, ebenso finden dort die Entwicklungen statt.

Seit SAP HANA 2.0 SPS1 werden nur noch Multi-Tenant-Datenbanken unterstützt. Erfolgt ein Update eines Single-Container-Systems auf ein Release >= 2.0 SPS1, wird das System in eine Multi-Tenant-Datenbank konvertiert.

Ein Multi-Tenant-System hat u. a. folgende Eigenschaften:

#### Benutzer- und Berechtigungsverwaltung

- Jeder Tenant hat eine eigene Benutzer- und Berechtigungsverwaltung.
- Den Benutzer SYSTEM gibt es in der Systemdatenbank sowie in allen Tenant-Datenbanken. In der Systemdatenbank verfügt er über erweiterte Rechte für tenant-übergreifende T\u00e4tigkeiten.
- Auf der Betriebssystemebene kann pro Tenant ein Benutzer definiert werden (siehe Abschnitt 4.5, »High Isolation Level für Tenants«).
- In der Systemdatenbank gibt es die Berechtigung DATABASE ADMIN für die Administration der Tenant-Datenbanken (siehe Abschnitt 4.1.1, »Berechtigungen zur Verwaltung von Tenants«).
- Berechtigungen sind nur innerhalb der jeweiligen Tenant-Datenbank gültig.
- Lesezugriffe zwischen Tenant-Datenbanken sind möglich, müssen aber explizit eingerichtet werden (siehe Abschnitt 4.2, »Tenant-übergreifende Zugriffe«). Standardmäßig sind sie deaktiviert.
- Authentifizierung und Single Sign-on
  - Die Authentifizierungs-Mechanismen können pro Tenant unterschiedlich eingesetzt werden.
  - Die Anmeldeparameter können individuell pro Tenant (Datei indexserver.ini) und Systemdatenbank (Datei namesever.ini) definiert werden.
- Verschlüsselung
  - Die Verschlüsselung der Kommunikation (Secure Sockets Layer, SSL) kann pro Tenant individuell konfiguriert werden.
  - Die Verschlüsselung der Dateien auf Betriebssystemebene kann pro Tenant konfiguriert werden.

#### Security Audit Log

 Das Security Audit Log (siehe Kapitel 11, »Auditing in SAP HANA«) kann pro Tenant konfiguriert werden. - Standardmäßig werden die Log-Einträge in einer lokalen Tabelle der Tenants gespeichert. Der lokale Tenant-Administrator kann dies nicht ändern (gemäß der Konfiguration in der Datei **multidb.ini**). Lediglich der Administrator der Systemdatenbank ist dazu berechtigt. Wird das Security Audit Log ins Unix-Systemprotokoll geschrieben, können die Einträge der verschiedenen Tenants über das Feld **Database Name** unterschieden werden.

Abbildung 4.1 zeigt den Aufbau einer Multi-Tenant-Datenbank. Die Systemdatenbank dient zur Verwaltung der gesamten Datenbank, daher sind hier als Benutzerkonten meist nur die Systemadministratoren eingerichtet. In den *Tenants* befinden sich die produktiven Prozesse. Auch hier gibt es Administratoren, die den Tenant verwalten. Sie haben aber keinen Zugriff auf andere Tenants oder die Systemdatenbank. Die Entwickler sind ebenfalls in den Tenants eingerichtet. Entwicklungen werden mit SAP HANA XSA erstellt. Und schließlich ist auch das Berechtigungskonzept tenantspezifisch. Rollen können in verschiedenen Tenants nur durch Export und Import ausgetauscht werden.



Abbildung 4.1 Aufbau einer Multi-Tenant-Datenbank

Die View M\_DATABASES listet die existierenden Tenants mit ihren Eigenschaften auf (siehe Abbildung 4.2). Sie muss in der Systemdatenbank aufgerufen werden. Wird sie in einem Tenant aufgerufen, wird nur der aktuelle Tenant als Eintrag angezeigt. Das Feld ACTIVE\_STATUS zeigt an, ob der Tenant gestartet, also erreichbar ist (Eintrag YES). Die Felder OS\_USER und OS\_GROUP zeigen Betriebssystembenutzer und -gruppe an, falls das Isolation Level auf »high« gesetzt ist (siehe Abschnitt 4.5, »High Isolation Level für Tenants«).

# **[\***]

## Weitere Informationen

Weiterführende Informationen zu Tenant-Datenbanken erhalten Sie im SAP HANA Tenant Databases Operations Guide.

SQL	Console 1.sql ×										
🔊 🖉 🔲 Analyze 🗸 🖳 '=, 🗹 Current schema: SYSTEM 🛛 Connected to: SYSTEMDB@HD3 (192.168.250.226:0) 🚿											
1 - select * from M_DATABASES											
Result ×     Messages ×       Rows (4)     SQL											
Rows	(4)					SQL	<u>↓</u> C	×,			
Rows	(4) DATABASE_NAME	DESCRIPTION V	ACTIVE_STATUS	ACTIVE_ST.	OS_USER 💌	SQL	⊥ C RESTAR	ی T_MODE			
Rows	(4) DATABASE_NAME V SYSTEMDB	DESCRIPTION V SystemDB-HD3-00	ACTIVE_STATUS *	ACTIVE_ST.	OS_USER V	SQL OS_GROUP V	✓ C     RESTAR     DEFAULT	× T_MODE			
Rows	(4) DATABASE_NAME Y SYSTEMDB HD3	DESCRIPTION V SystemDB-HD3-00 HD3-00	ACTIVE_STATUS V YES YES	ACTIVE_ST	OS_USER 💌 NULL hd3usr	SQL OS_GROUP V NULL hd3grp	L     C     RESTAR     DEFAULT     DEFAULT	S T_MODE			
Rows	(4) DATABASE_NAME Y SYSTEMDB HD3 HD4	DESCRIPTION 👻 SystemDB-HD3-00 HD3-00 NULL	ACTIVE_STATUS Y YES YES YES	ACTIVE_ST.	OS_USER V NULL hd3usr hd4usr	SQL OS_GROUP V NULL hd3grp hd4grp	✓ C     RESTAR     DEFAULT     DEFAULT	× T_MODE T			

Abbildung 4.2 View M\_DATABASES

## 4.1.1 Berechtigungen zur Verwaltung von Tenants

Die Verwaltung der Tenants erfolgt von der Systemdatenbank aus. Von hier aus können Tenants angelegt, gelöscht und umbenannt werden. Auch das Starten und Stoppen erfolgt von hier aus. Tabelle 4.1 zeigt die System Privileges, die zur Verwaltung der Tenants erforderlich sind. Diese Privileges gibt es nur in der Systemdatenbank.

System Privilege	Beschreibung
DATABASE ADMIN	Berechtigt zur Verwaltung der Tenants (Anlegen, Ändern, Löschen, Backup, Recovery): CREATE DATABASE ALTER DATABASE DROP DATABASE RENAME DATABASE BACKUP DATABASE RECOVERY DATABASE BACKUP CHECK BACKUP LIST DATA
DATABASE START	Berechtigt zum Starten aller Tenant-Datenbanken: ALTER SYSTEM START DATABASE
DATABASE STOP	Berechtigt zum Stoppen aller Tenant-Datenbanken: ALTER SYSTEM STOP DATABASE

Tabelle 4.1 Berechtigungen zur Tenant-Verwaltung

# 4.1.2 Verwaltung von Tenants mit dem SAP HANA Cockpit

Die Verwaltung von Tenants (Abbildung 4.4) erreichen Sie im SAP HANA Cockpit über das Resource Directory (Kachel **Resource Directory**). Zu allen Systemdatenbanken wird der Link **Manage Databases** angezeigt (siehe Abbildung 4.3). Den Link finden Sie auch jeweils im Fenster **System Overview** der Systemdatenbanken.

A C 🗥 SAP SYSTEMDB@H4S	system)	Reso	urce Dire	ctory $\checkmark$				3
efault 🗠								Manage Resou
Search Q All	~ A	1		∼ All			∽ All	$\sim$
06:								
dl 🗸 🗸							Restore	e Adapt Filters
			~					
Resources (7)							Gro	oup by System 🛛 {
Status Resource Description	Alert	Grou	Availabil	Performanc	Capacit	Ilsano	Credentials	SAP Control
	S	р	ity	e	У	00030	orodonilaio	Credentials
SYSTEMDB@H4S		4	A			Teat	User: system	
Manage Databases	<u> </u>		(13)	Ŷ	<b>V</b>	lest	Manage Credentia	als Enter Credential
Type/Version:								
SAP HANA SYSTEM Database								
2.00.030.00.1522209842 (fa/hana2sp03)								
SYSTEMDB@H4C							User: system	
Running 192.168.10.23 Manage Databases		1	*	$\checkmark$	1	Custom	Manage Credentia	als Enter Credential
Traction								
Typer version.								
SAP HANA SYSTEM Database								

## Abbildung 4.3 Aufruf der Tenant-Verwaltung im SAP HANA Cockpit

8	<	ŝ	SAP	SYSTEMDB	Manag	ge Database	s ∨				3	Ç	
H4S										Manage Blacklisted	Parameter	rs	
Overall S	Status:	All data	abases running										
Isolation Descript	Level: tion:	Low											Ń
						$\sim$							
Data	ıbase	s (2)				Search		Q	Create Tenant	Back Up Tenant	↑↓	$\diamond$	
Statu	s	Data	base Name	Start Time	Used Memo	ory	Disk Usag	Ю		Fallback Snapsho	t Action		
🗖 R	unning	SYS	TEMDB	Nov 13, 2018, 10:00:19 AM	_	I	-			Not supporte	d		
🗖 R	unning	H4S		Nov 13, 2018, 10:00:33 AM		1	_			No snapsho	st Stop	Tenant	

### Abbildung 4.4 Verwaltung der Tenants

In der Statuszeile können Sie über die Schaltfläche **More** (**Jose**) die Pflege der Blacklisted Parameter (siehe Abschnitt 4.3, »Nicht änderbare Parameter in Tenants«) sowie die Pflege der Restricted Features (siehe Abschnitt 4.4, »Einschränkung von Funktionen in Tenants«) aufrufen. Im Bereich **Databases** legen Sie mit dem Link **Create Tenant** einen neuen Tenant an. Hier haben Sie zwei Möglichkeiten:

- Anlegen eines leeren Tenants
- Anlegen eines Tenants als Kopie eines bestehenden Tenants. Hiermit ist auch ein Verschieben möglich. Die Tenants können systemübergreifend kopiert werden, also von einer SAP-HANA-Datenbank in eine andere.

Bei der Anlage eines neuen Tenants geben Sie einen Namen für den Tenant sowie das Kennwort für den Benutzer SYSTEM ein (siehe Abbildung 4.5). Der Tenant wird angelegt und in der Sicht **Manage Databases** angezeigt (Abbildung 4.6). Wurde die Option **Start Automatically** gesetzt, wird der Tenant sofort gestartet, und Anmeldungen sind mit dem Benutzer SYSTEM möglich. Hierfür kann der Tenant in das Resource Directory des SAP HANA Cockpits eingebunden werden.

8 <b>&lt; Sap</b>	Manage Databases $\vee$	3	C
General Settings			
*Database Name:	HD5		
*SYSTEM User Password:	•••••		
*Confirm Password:	•••••		
Start Automatically:	$\checkmark$		
> Advanced Settings			
		Create Tenant Database	Cancel

Abbildung 4.5 Anlegen eines neuen Tenants

Abbildung 4.6 zeigt das Menü mit den möglichen Aktionen für die Tenants. Von hier aus können Backup und Recoveries durchgeführt und die Tenants kopiert bzw. repliziert werden.

## [\*]

#### Weiteres Informationen zu Backups und Recoveries

Detaillierte Beschreibungen zu Backups und Recoveries finden Sie im SAP HANA Administration Guide und im SAP HANA Tenant Databases Operations Guide.

8 < 6	SAP SYSTEMD	Manag	ge Databases 🗸			3 (	2
HD3					Manage Blacklisted Para	ameters	•
			$\sim$				
Databases (4)			Search	Q Create Tenant	Back Up Tenant	^↓ {	3
Database Name	Start Time	Used Memory	Disk Usage		Fallb: Recover Tenant		
SYSTEMDB	Dec 20, 2018, 9:50:48 AM				Delete Tenant		
HD5	Jan 28, 2019, 11:10:02 AM	-			Rename Tenant		
HD4	Dec 23, 2018, 4:02:21 PM				Copy Tenant		
HD3	Dec 20, 2018, 9:50:59 AM		_		Replicate Tenant Set Restart Mode	e	
					Create Fallback	Snapshot	
					Delete Fallback	Snapshot	
					Reset to Fallback	< Snapsho	t
					Reset SYSTEM P	Password	

Abbildung 4.6 Verwaltung der Tenants

#### 4.1.3 Verwaltung von Tenants mit SAP HANA XSA

Tenants können auch mit dem SAP HANA XSA Cockpit angelegt und gelöscht werden. Der Vorteil besteht darin, dass sie hier für die Nutzung in SAP HANA XSA aktiviert werden können. Des Weiteren können hier den Tenants Organizations und Spaces direkt zugeordnet werden.

Rufen Sie zur Verwaltung den Eintrag **Tenant Databases** im SAP HANA XSA Cockpit auf (siehe Abbildung 4.7).



Abbildung 4.7 Tenant-Verwaltung im SAP HANA XSA Cockpit

Hier werden zu den bestehenden Tenants auch bereits die zugeordneten Organizations und Spaces angezeigt. Klicken Sie auf **New Tenant Database**, um einen neuen Tenant anzulegen. Geben Sie die Daten für den neuen Tenant ein (siehe Abbildung 4.8).



Abbildung 4.8 Anlage eines neuen Tenants

Nach der Anlage wird der neue Tenant in der Übersicht angezeigt. Klicken Sie zur Aktivierung des Tenants für SAP HANA XSA auf die Schaltfläche **Enable Tenant** (). Im nächsten Schritt können Sie die Organizations und Spaces zuordnen. Dies erfolgt mit der Schaltfläche **Allocate Tenant** (). Wählen Sie die Organizations und Spaces aus (siehe Abbildung 4.9). Diese werden dem Tenant zugeordnet (Abbildung 4.10).



Abbildung 4.9 Zuordnung von Organizations und Spaces zum Tenant



Abbildung 4.10 Neuer Tenant mit zugeordneten Organizations und Spaces

## 4.2 Tenant-übergreifende Zugriffe

Standardmäßig sind tenant-übergreifende Zugriffe deaktiviert. Gesteuert wird die Möglichkeit des Zugriffs über folgenden Systemparameter:

Datei global.ini • cross\_database\_access - enabled

Dieser Parameter kann standardmäßig nur von der Systemdatenbank aus gesetzt werden. Ein Zugriff ist grundsätzlich auf SELECT-Statements eingeschränkt, also nur lesend. Um den Zugriff auf einen anderen Tenant zu ermöglichen, müssen Benutzern sogenannte *Remote-Benutzer* in den anderen Tenants zugeordnet werden. Die entsprechende Beschreibung finden Sie in Abschnitt 6.4, »Remote-Benutzer«.

## 4.3 Nicht änderbare Parameter in Tenants

Einige Systemeigenschaften sollten nur von der Systemdatenbank aus geändert werden können. Hierzu gehören z. B. Änderungen an der Einstellung der Verschlüsselung der Kommunikation, der Speicherverwaltung und der Systemreplikation. Dies wird über Systemparameter gesteuert. Für die Parameter kann gesteuert werden, ob sie nur in der Systemdatenbank oder auch in Tenant-Datenbanken geändert werden können. Dies erfolgt über die Datei **multidb.ini**, Abschnitt readonly\_parameters. Sie können diese Einstellungen auch in der Tenant-Verwaltung des SAP HANA Cockpits pflegen. Klicken Sie hierfür auf die Schaltfläche **Manage Blacklisted Parameters**. Sie gelangen in die Sicht **Blacklisted Parameters for Tenants** (siehe Abbildung 4.11). Hier können Sie mit der Schaltfläche **Add Parameter** weitere Parameter hinzufügen, die in Tenant-Datenbanken nicht gepflegt werden sollen. Hierfür ist das System Privilege INIFILE ADMIN erforderlich.

A K 🏠 SAP SY	STEMDB@HD3 (	Bl	acklisted & Restricted $ \smallsetminus $	3
Tenants			Blacklisted Parameters for Tenants	[/ Open In
Search C	Blackliste	d Parameters	HD3 system Search Q Add Param	eter Copy Parameters ↑↓
nbo system	File	Section	Parameters	Layer
HD3@HD3		auditing configurati on	default_audit_trail_type,emergency_audit_trail_type,alert_audit	DEFAULT
HD4@HD3		communic ation	*	DEFAULT
HD5@HD3		execution	max_concurrency	DEFAULT
		memorym anager	$allocation limit, minallocation limit, global\_allocation\_limit, a sync\_fr\dots$	DEFAULT
		session	maximum_connections,maximum_external_connections	DEFAULT
		sql	sql_executors	DEFAULT
	global.ini	customiza ble_functi onalities		DEFAULT
		extended_ storage	*	DEFAULT
		persistenc e	basepath_datavolumes_es,basepath_logvolumes_es,basepath	DEFAULT
		system_re plication	keep_old_style_alert,enable_full_sync,operation_mode	DEFAULT
		system_re plication_ communic		DEFAULT

Abbildung 4.11 Pflege der Blacklisted Parameter

# 4.4 Einschränkung von Funktionen in Tenants

SAP HANA stellt viele Funktionen zur Verfügung, die aus Sicherheitsaspekten nur in der Systemdatenbank ausgeführt werden sollten. Dazu können z.B. die Durchführung von Backups und die Verwaltung des externen Speichers gehören. Daher ist es möglich, Funktionen für Tenants zu sperren. Im SAP HANA Cockpit erreichen Sie die Konfiguration über die Tenant-Verwaltung, Schaltfläche **Manage Restricted Features** (siehe Abbildung 4.12).

Standardmäßig sind alle Features für alle Tenants aktiviert. Je nach Systembetrieb konfigurieren Sie die Einstellungen für jeden Tenant. Werden z. B. die Backups der Tenants grundsätzlich von der Systemdatenbank ausgeführt, deaktivieren Sie den Punkt **BACKUP**. Auch die Befehle **IMPORT** und **EXPORT** können für die Tenants deaktiviert werden, sodass z. B. sensible Daten nicht in das Dateisystem des Servers exportiert werden können.

A K 🏠 SAP SYSTE	MDB@HD3 (system) Blacklisted & Restricted $\sim$		3
Tenants	Restricted Features	s for Tenants	[උ Open In
Search Q	Select which features to restrict for tenant HD3@HD3	Search Q Copy R	estricted Features
	E Feature	Description	Layer
HD3@HD3	ACCELERATOR_FOR_ASE	SAP HANA Accelerator for SAP ASE operations	DEFAULT
HD4@HD3	AFL AFL	Access to Application Function Libraries (AFL) for business logic in native C++	DEFAULT
HD5@HD3	✓ ALTERSYSTEM	Execution of ALTER SYSTEM statements	DATABA 🛞 SE
		Execution of the statement ALTER SYSTEM RECONFIGURE SERVICE, which re-reads the service configuration	DATABA 🛞 SE
	SACKUP	Backup Operations	DATABA 🛞 SE
	☑ IGNORE_PATH_RESTRICT	lgnoring of path restrictions for Backup Operations	DATABA ⊗ SE
	BOE	BO Explorer API	DEFAULT
	BUILTINPROCEDURE	Execution of procedures associated with critical and/or optional functions	DEFAULT
	BW CONVERT CLASSIC TO IMO CUBE	Operation of an SAP BW powered by SAP HANA	DEFAULT

Abbildung 4.12 Einschränkung von Funktionen in Tenants

Werden Funktionen deaktiviert, so werden sie als Parameter in die Datei **global.ini**, Abschnitt customizable\_functionalities, eingetragen. In Abbildung 4.12 sind vier Funktionen für das System HD3 deaktiviert:

- ALTERSYSTEM
- ALTERSYSTEM.RECONFIGURE SERVICE
- BACKUP
- BACKUP.IGNORE\_PATH\_RESTRICT

Diese vier Funktionen finden sich als Parameter wieder (siehe Abbildung 4.13). Hierüber können auch Funktionen deaktiviert werden, die nicht im Standard in der Sicht **Manage Restricted Features** enthalten sind. Sie können direkt als neuer Parameter im Abschnitt customizable\_functionalities eingetragen werden.

Die Einstellung der deaktivierten Funktionen kann mit zwei Views eingesehen werden. In Tenants kann die View M\_CUSTOMIZABLE\_FUNCTIONALITIES (Schema SYS) genutzt werden. Diese zeigt für den aktuellen Tenant die Einstellung zu den Funktionen an. In der Systemdatenbank kann die View SYS\_DATABASES.M\_CUSTOMIZABLE\_FUNCTIONALI-TIES genutzt werden. Diese enthält die Einstellungen aller Funktionen in allen Tenants. Abbildung 4.14 zeigt diese View. Die beiden markierten Datensätze zeigen an, dass sie im Tenant H4S deaktiviert sind (Spalte IS\_ENABLED = FALSE).

182

å <b>&lt;</b> å	SAP	Configuration of System Properties V								
Search Database:	Configuration F Q global.ini	ïle: ✓	Section: customizable_functionali	Host All						
Configuration File Co	intents			Ac	d Section					
Section	Parameter	Layer	Specific Value							
[] customizable _functionaliti es	altersystem	DATABASE (HD3)	false	Edit Specific Value	*					
	altersystem.reconfigure_servic	e DATABASE (HD3)	false	Edit Specific Value	8					
	backup	DATABASE (HD3)	false	Edit Specific Value	$\otimes$					
	backup.ignore_path_restrict	DATABASE (HD3)	false	Edit Specific Value	$\otimes$					
		DEENUT		Chapao Lava						

Abbildung 4.13 Eingeschränkte Funktionen in der Datei »global.ini«

SQL 0	Console 1.sql ×											
0	🔲 Analyze 🗸	⊥ ·=, 🗹 Current schema: TT	EDE Connected to: SYSTEMDB@H4S (192.	68.225.25:2)								
1 * s	1 * select * from SYS_DATABASES.M_CUSTOMIZABLE_FUNCTIONALITIES											
Result	× Messages ×											
Rows (	(96)		SQL	<u>+</u> C >								
	DATABASE_NAME	NAME	DESCRIPTION	IS_ENABLED								
45	SYSTEMDB	LDAP	LDAP Operations	TRUE								
46	SYSTEMDB	PLANNINGENGINE	Planning Engine features	TRUE								
47	SYSTEMDB	EPMPLANNING	SAP HANA Enterprise Performance Manag	TRUE								
48	SYSTEMDB	RINTEGRATION	Rlanguage	TRUE								
49	H4S	XB_MESSAGING_SUBSCRIPTIONS	Subscriptions For External Messaging Prov	TRUE								
50	H4S	AFL	Access to Application Function Libraries (A	TRUE								
51	H4S	BACKUP	Backup Operations	FALSE								
52	H4S	BACKUP.IGNORE_PATH_RESTRICT	Ignoring of path restrictions for Backup Ope	FALSE								
53	H4S	IMPORTEXPORT	Import Export Operations	TRUE								
54	H4S	IMPORTEXPORT.IMPORT	Import Operations	TRUE								
55	H4S	IMPORTEXPORT.EXPORT	Export Operations	TRUE								
56	H4S	IMPORTEXPORT.IGNORE_PATH_RESTR	Ignoring of path restrictions for import and	TRUE								

Abbildung 4.14 Die View SYS\_DATABASES.M\_CUSTOMIZABLE\_FUNCTIONALITIES

# 4.5 High Isolation Level für Tenants

Standardmäßig läuft eine SAP-HANA-Datenbank unter einem einzigen Betriebssystembenutzer, dem Benutzer <sid>adm (siehe Abschnitt 2.1.2, »Benutzer <sid>adm«). Dies ist das Isolation Level »low«, der Standard für SAP-HANA-Datenbanken. Das bedeutet, dass dieser Benutzer Zugriff auf die Daten aller Tenants hat, die im Betriebssystem gespeichert werden, z. B.:

- Backups
- Redo-Logs
- Log-Dateien
- Datendateien (z. B. persistente Daten)

Handelt es sich dabei um hochsensible Daten, besteht die Anforderung, dass die Daten von den Tenant-Administratoren verwaltet werden und nicht von den Systemadministratoren, welche die Systemdatenbank betreuen.

Hierfür besteht die Möglichkeit, tenant-spezifische Betriebssystembenutzer und -gruppen anzulegen (Isolation Level »high«). Die Verwaltung der Daten im Betriebssystem kann somit auf unterschiedliche Personenkreise aufgeteilt werden. Damit geht einher, dass die systeminterne Kommunikation nur noch verschlüsselt stattfinden darf. Die Vorgehensweise hierbei ist folgende:

- 1. Im Betriebssystem werden für alle Tenants jeweils ein tenant-spezifischer Benutzer und eine Gruppe angelegt.
- 2. Alle Tenants müssen gestoppt und per Skript im Betriebssystem auf den High-Isolation-Modus gesetzt werden.
- 3. Den Tenants werden die zuvor angelegten Betriebssystembenutzer und -gruppen zugeordnet.
- 4. Die Tenants werden wieder gestartet.

Danach werden die Daten der Tenants im Betriebssystem mit den Berechtigungen dieser Benutzer und Gruppen gespeichert. Mit den einzelnen Benutzern ist daher nur der Zugriff auf die jeweiligen Tenant-Daten möglich. Abbildung 4.15 zeigt die Benutzer und Gruppen der Systemdatenbank und der Tenants.

Im ersten Schritt müssen die Benutzer und Gruppen für die Tenants angelegt werden. Im System, in dem hier beispielhaft das Isolation Level »high« eingerichtet werden soll, existieren neben der System-DB die drei Tenants HD3, HD4 und HD5. Tabelle 4.2 zeigt, welche Benutzer und Gruppen für die Tenants genutzt werden sollen.

Tenant	BS-Benutzer	BS-Gruppe
HD3	hd3usr	hd3grp
HD4	hd4usr	hd4grp
HD5	hd5usr	hd5grp

 Tabelle 4.2
 Benutzer und Gruppen f
 ür das Isolation Level »high«

## SAP HANA Multi-Tenant-Datenbank – Isolation Level High



Abbildung 4.15 Betriebssystembenutzer und -gruppen im High Isolation Level

Mit dem Kommando groupadd <Gruppe> werden zuerst die Gruppen angelegt. Danach werden die Benutzer mit folgendem Kommando angelegt:

useradd -g sapsys <Benutzer>

Dies bewirkt, dass der neue Benutzer der Gruppe sapsys zugeordnet wird. Im nächsten Schritt müssen die Benutzer der Gruppe <sid>shm sowie der Gruppe ihres Tenants zugeordnet werden:

usermod -G <sid>shm,<Tenant-Gruppe> <Benutzer>

#### Abbildung 4.16 zeigt die Befehle für alle drei Tenants.



Abbildung 4.16 Anlage von Gruppen und Benutzern

Als Nächstes ist das Isolation Level »high« per Skript über das Betriebssystem einzustellen. Dafür müssen die Tenant-Datenbanken gestoppt werden. Dies kann über das SAP HANA Cockpit in der Sicht **Manage Databases** erfolgen. Abbildung 4.17 zeigt, dass die drei Tenants gestoppt sind. Um das Isolation Level zu setzen, ist eine Anmeldung an das Betriebssystem mit dem Benutzer <sid>adm erforderlich. Mittels des Python-Skripts **convertMDC.py** wird nun das Isolation Level »high« gesetzt. Das Skript wird folgendermaßen aufgerufen:

python /usr/sap/<sid>/HDB<Instanz>/exe/python\_support/convertMDC.py
--change=databaseIsolation --isolation=high

#### In unserem Beispiel folgendermaßen:

python /usr/sap/HD3/HDB00/exe/python\_support/convertMDC.py
--change=databaseIsolation --isolation=high

Das Skript stoppt zuerst die SAP-HANA-Datenbank und setzt dann das Isolation Level »high«. Danach wird die Datenbank wieder gestartet. Abbildung 4.18 zeigt die Ausgabe des Skripts.

8	<	â	SAP	SYSTEME	) <b>N</b>	/lanage [	Databases N	1				3	C	
HD3										Manage Blackliste	d Para	meters		
Overall Isolation Descrip	Status: n Level: otion:	3 data 1 data Low	ibases stopped abase running v	l vith issues										Ŕ
						1								
Data	abase	s (4)				Search		Q	Create Tenant	Back Up Tenant		$\uparrow_{\downarrow}$	٢	
Data Nam	base e			Start Time	Used Memory		Disk Usaç	je		Fallback Snap	shot	Action		
HD3										No snap:	shot	Start "	Tenant	
HD4										No snap:	shot	Start -	Fenant	
HD5										No snaps	shot	Start	Fenant	
SYS	TEMD	З (	Dec 20, 2018, 9	9:50:48 AM						Not suppo	rted			

#### Abbildung 4.17 Stoppen der Tenant-Datenbanken

Durch das Skript ist nun auch der Parameter database\_isolation (Datei global.ini, Abschnitt multidb) auf den Wert »high« gesetzt. Es fehlt nun noch die Zuordnung der Betriebssystembenutzer und -gruppen zu den Tenants. Dies kann mit dem Befehl ALTER DATABASE <Tenant> OS USER '<Betriebssystembenutzer>' OS GROUP '<Betriebssystemgruppe> erfolgen oder mit dem SAP HANA Cockpit in der Sicht Manage Databases. Wählen Sie einen Tenant aus, und wählen Sie über die Schaltfläche More () den Eintrag Assign OS User and OS Group aus.



Abbildung 4.18 Ausgabe des Python-Skripts convertMDC.py

Geben Sie Benutzer und Gruppe für die Tenants an (Abbildung 4.19). Danach können die Tenants über die Schaltfläche **Start Tenant** wieder gestartet werden. In der Übersicht lassen sich dann über die Schaltfläche **Settings** (③) zu den Tenants auch die Betriebssystembenutzer und -gruppen anzeigen (siehe Abbildung 4.20).

<	SA	P	Manag	je Databases				3	Ċ
HD3									
Overall :	Status n Leve	s: 3 databas 1 databas I: High	es stopped Assign O	S User & OS G	roup				
			Specify an existing OS user	and group for this	tenant database	. Assic	p Tenant 1: fallback Snapshot / No snapshot ( No snapshot (		Ś
Databases (4)		(4)	tenant to a dedicated OS user and group secures internal communication level is high.			Ip Tenant 🛛 🔐	↑↓ @		
Databas Name	e		*OS User:	hd3usr			allback Snapshot	Action	
HD3			*OS Group:	hd3grp			No snapshot	Start Te	enant
HD4					OK	Cancel	No snapshot	Start Te	enant
HD5							No snapshot	Start Te	enant
SYSTEN DB	N	Jan 28, 20	19, 3:56:42 PM				Not supported		

Abbildung 4.19 Zuordnung von Betriebssystembenutzer und -gruppe zum Tenant

a K Sap	Man	age Databases $\vee$				3 C				
HD3						***				
Databases (4)	Sear	ch Q	Create Tenant Back Up Tenant			↑↓ ۞				
Database Name	Start Time	Used Memory		OS User	OS Group	Action				
SYSTEMDB	Jan 28, 2019, 3:56:42 PM		1	I						
HD5	Jan 28, 2019, 4:59:32 PM		I	hd5usr	hd5grp	Stop Tenant				
HD4	Jan 28, 2019, 4:59:55 PM	-	I	hd4usr	hd4grp	Stop Tenant				
HD3	Jan 28, 2019, 4:58:58 PM	-	I	hd3usr	hd3grp	Stop Tenant				

Abbildung 4.20 Tenants mit Betriebssystembenutzer und -gruppe

# 4.6 Protokollierung von Änderungen an Tenants

Die Pflege von Tenant-Datenbanken kann über das Auditing (siehe Kapitel 11, »Auditing in SAP HANA«) protokolliert werden (siehe Abbildung 4.21). Folgende Aktionen können protokolliert werden:

- Anlegen, Ändern und Löschen von Tenant-Datenbanken
- Umbenennen von Tenant-Datenbanken
- Starten und Stoppen von Tenant-Datenbanken



Abbildung 4.21 Protokollierung von Änderungen an Tenants

Da diese Aktionen nur von der Systemdatenbank aus ausgeführt werden können, lässt sich diese Protokollierung nur dort einrichten. In Tenant-Datenbanken sind diese Aktionen im Auditing nicht verfügbar.

Des Weiteren können auch Änderungen an den Einstellungen zur Verschlüsselung tenant-spezifisch protokolliert werden (siehe dazu Abschnitt 3.3.8, »Protokollierung von Änderungen an der Verschlüsselung«).