Aspekte des Berechtigungs-managements für SAP HANA

Ergänzte Neuauflage des Best-Practices-Leitfadens „Rollenmanagement in SAP HANA“ v2

Stand: Februar 2021

Autoren

Kürzel	Name	E-Mail	Unternehmen
TT	Thomas Tiede	Thomas.Tiede@ibs-schreiber.de	IBS Schreiber GmbH
MvB	Martin van Baal	Martin.van-Baal@postbank.de	Postbank
SL	Stephanie Lewellen (SAP)	stephanie.lewellen@sap.com	SAP SE
LS	Levente Szelitzky	levente.szelitzky@db.com	Deutsche Bank AG
TF	Thorsten Füg	thorsten.fueg@pagnos.com	Pagnos GmbH
CK	Christian Koch	christianbt_koch@gmx.de	Sycor GmbH
JL	Jan Lange	jan.lange@miele.com	Miele & Cie. KG
BW	Benjamin Wegener	benjamin.wegener@ucc.ovgu.de	SAP University Competence Center Magdeburg
BB	Bert Braasch	bert.braasch@in4md-service.de	in4MD Service GmbH

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung

SAP liefert zum Thema Sicherheit unter SAP HANA bereits eine sehr umfangreiche Dokumentation. Dennoch gibt es in der Praxis immer wieder Konstellationen, die konzeptionell noch nicht abgedeckt werden. Zudem ist die Dokumentation von SAP mit Fokus auf allgemeine Gültigkeit erstellt worden. Das führt bei Anwendern mitunter zu Schwierigkeiten oder Unsicherheiten, wie die Empfehlungen sinnvoll in ein betriebsnahes Konzept überführt werden können. Es besteht der Wunsch nach einer Orientierungshilfe, einer Art „rotem Faden“.

Gerade in den Themengebieten rund um ein Berechtigungskonzept gilt es zu Anfang, einige strategische Entscheidungen zu treffen, um ein solides und praxistaugliches Endergebnis zu erhalten. Der vorliegende Leitfaden repräsentiert eine mit SAP abgestimmte Zusammenführung verschiedener Best-Practice-Ansätze und -Lösungsvorschläge aus Sicht von Kunden und Beratern, die SAP HANA bereits erfolgreich im Einsatz betreiben. Ergänzend zu den bestehenden Dokumentations-referenzen von SAP erhalten IT-Sicherheitsexperten die notwendige Unterstützung zur Implementierung eines Berechtigungskonzepts unter SAP HANA in den unterschiedlichsten Ausgangslagen.

Die zweite Auflage des Leitfadens hat eine erhebliche Ergänzung erfahren. Sie ist um mehrere Kapitel erweitert worden und umfasst Themen, die es nicht in die erste Auflage geschafft haben bzw. welche seitdem in weiteren Arbeitssitzungen ausgearbeitet wurden. Themen wie Massenoperationen, Berechtigungsebenen und Notfallbenutzer kamen hinzu. Auf XSA ist weiterhin wenig Fokus gelegt worden, was vor allem den immer noch bescheidenen Erfahrungswerten mit produktiven XSA-Umgebungen geschuldet ist.

Das Autorenteam erhofft sich, dass die aktualisierte Version zumindest einen neuen Impuls für die Diskussion zu diesem wichtigen Themenkomplex in der DSAG geben kann.

1 Rollenmanagement

1.1 Designzeitrollen

Es wird allgemein als Best Practice angesehen, möglichst die Einzelberechtigungen ausschließlich über Rollen einem Benutzer (personalisiert sowie technisch) zuzuweisen. Hierzu werden mit Ausnahme der folgenden Bereiche immer Designzeitrollen (Berechtigungen sind vom Benutzer entkoppelt und transportierbar) verwendet.

Ausnahmen (was kann ausschließlich in Laufzeitrollen abgebildet werden):

- SAP HANA, intelligenter Datenzugriff (SAP HANA Smart Data Access): Eine Remote-Source-bezogene Anlage von Objekten, wie z. B. virtuellen Tabellen, kann zunächst nur vom Besitzer der Remote Source durchgeführt werden. Die Vererbung der Berechtigungen auf die Remote Source kann von dem Besitzer direkt an die Benutzer vorgenommen werden, wobei das keinen Best-Practice-Ansatz darstellt und unter anderem den Nachteil des erhöhten Pflegeaufwands mit sich bringt. Die nachhaltige und bessere Methode beinhaltet die Anlage und die Vererbung dieser Berechtigungen an eine dafür über einen technischen Benutzer angelegte Laufzeitrolle.
- BW on HANA: Rollen, die über die Applikation in der Datenbank generiert werden, sind im Standard Laufzeitrollen. Die Berechtigung von BW-generierten Objekten ist, da über die Applikation verwaltet und vorgegeben, nur über die erwähnten Laufzeitrollen oder über eine direkte Benutzerzuordnung der Berechtigungen möglich.
- SAP HANA smart data integration (<= Rev. 122): Aktivierung der Flow-Graphen und Replication-Tasks, die Verarbeitung von Remote-Subscription-Exceptions
- Erstellung administrativer Benutzer (Rollenerstellung in XS Classic): Benutzer, die Berechtigungen weitergeben dürfen sollen, können diese nicht über eine Designzeitrolle erhalten. Die Option „Grantable to Others“ ist beim Erstellen einer Designzeitrolle unter XS Classic nicht verfügbar.
- Berechtigung zum Debuggen der Session eines anderen Benutzers (z. B. SAPSID): Die Berechtigung „Attach Debugger“ unter dem Reiter „Privileges on User“ kann nur vom betroffenen Benutzer selbst in einer Laufzeitrolle oder auf Benutzerebene gesetzt werden und ist beim Erstellen einer Designzeitrolle nicht verfügbar.
- Die Verwendung von Benutzergruppen: Eine Benutzergruppe (verfügbar seit SAP HANA 2.0 SPS02) kann aktuell ausschließlich einer Laufzeitrolle per ALTER-Statement zugewiesen werden.

- Rollenprovisionierung über das Active Directory (verfügbar seit SAP HANA 2.0 SPS03): Sollen Rollen per Active Directory vergeben werden, müssen diese als Laufzeitrolle implementiert werden. Das Mapping auf die entsprechenden AD-Gruppen kann aktuell nur über ein ALTER-Statement vorgenommen werden.
- Sammelrolle für _SYS_REPO-Benutzer (Rollenerstellung in XS Classic): Soll der _SYS_REPO-Benutzer neben dem Aspekt der übersichtlicheren Berechtigungsvergabe von den vergebenen Berechtigungen in jedem System auf dem gleichen Stand gehalten werden, kann eine Sammelrolle, die alle vom Standard abweichenden, zusätzlich hinzugefügten Berechtigungen beinhaltet, helfen. Da der _SYS_REPO-Benutzer jedoch in vielen Fällen die berechtigungsrelevante Option „Grantable to Others“ benötigt, kann das in XS Classic nur über eine Laufzeitrolle implementiert werden.

Die Handhabung der Ausnahmen könnte unter anderem wie folgt geregelt werden:

- Erstellung der Laufzeitrollen immer über technischen Benutzer
- manuell (muss auf jedem System manuell per SQL-Editor ausgeführt werden) oder per SQL-Script-Prozedur (kann transportiert werden) teilautomatisierte Erstellung
- Einbettung der Laufzeitrolle in eine Designzeitrolle (Wrapper), um diese auch ohne ROLE-ADMIN-Systemberechtigung vergeben und entziehen zu können

Bei der Aufteilung der Rollen kann generell folgendes Layout (selbstverständlich bei Bedarf auch differenzierter abzubilden) herangezogen werden:

Entwicklung:

- Entwickler auf Entwicklungssystemen
- Support-Benutzer auf allen Nichtentwicklungssystemen

Administration:

- Rollenadministrator (Erstellen von Rollen)
- Benutzeradministrator (Erstellen von Benutzern und Zuweisen der Rollen)
- Audit-Administrator (Audit-Konfiguration/-Überwachung)
- Datenbankadministrator (Datenbankkonfiguration sowie Konfiguration von Sicherheitseinstellungen/Passwortrichtlinien und Überwachung der Systeme)

1.2 SAP-Standardrollen

Mit den von SAP mitgelieferten Standardrollen wird wie folgt umgegangen.

Laufzeit:

- Die PUBLIC-Rolle z. B. wird komplett in eine eigene Rolle überführt (HANA-1.0-Restricted-Benutzer vorausgesetzt). Einige Laufzeitrollen wie die eben genannte PUBLIC-Rolle haben mehrere hundert Privilegien. Um die inhaltliche Überführung zu erleichtern, können die Laufzeitrollen über die Tabelle sys.effective_privileges ausgewertet werden. Nach der Aufbereitung dieser Privilegien in der passenden Syntax sind diese in eine Designzeitrolle einzufügen.
- Sie werden, falls notwendig (z. B. PUBLIC), 1 : 1 in den eigenen Rollen referenziert.

Designzeit:

- Die für Web-Applikationen mitgelieferten Rollen werden, falls möglich (in der Applikation bzgl. Prüfung nicht hart im Coding verankert), komplett in eigene Rollen überführt oder in den eigenen Namensraum kopiert.
- Sie werden nach Prüfung auf kritische Berechtigungen 1 : 1 in den eigenen Rollen referenziert. Falls kritische Berechtigungen vorhanden sind, SAP-Meldung aufmachen und vorerst abgespeckt in eigene Rolle überführen.

Um die Rollen aktuell zu halten bzw. teilautomatisiert auf Änderungen prüfen zu können, kann für die Metadaten auf SYSTEM-Views zurückgegriffen oder in den Security Guides/What's-new-Dokumenten nach Änderungen recherchiert werden.

1.3 Ablagestruktur

SAP rät ausdrücklich davon ab, Entwicklungsobjekte im SAP-Namensraum (sap-Paket) einer HANA-Instanz abzulegen, seien es Rollen, Analyseberechtigungen oder SAP HANA Extended Application Services und Classic-Model-Applikationen (XSC). Die Empfehlung ist daher, unter dem root-Paket einen kundeneigenen Namensraum in Form eines eigenen Pakets einzurichten, in dem alle eigenen Entwicklungen in Zusammenhang mit HANA und der XSC abgelegt werden.

Im Zuge der Rollenentwicklung empfiehlt es sich, ein Paket „sicherheit" anzulegen, das wiederum, je nach eigenem Bedarf, die Unterpakete für „rollen", „privilegien" und/oder „prozeduren" umfasst.

Nach eigenen Anforderungen kann ein solches sicherheit-Paket darüber hinaus pro Applikation eingerichtet werden, um applikationsspezifische Security-Objekte abzulegen und gemeinsam mit der Applikation transportierbar zu machen.

Die Paketstruktur sieht dann exemplarisch wie folgt aus:

root

sap
<Kundenpaket>
<Applikation1>
sicherheit
…
<Applikation2>
sicherheit
rollen
privilegien
prozeduren

Es bleibt dem Kunden überlassen, ob weitere Unterteilungen in der Paketstruktur vorgenommen werden, etwa in zu transportierende und lokale Pakete, die Unterteilung nach der jeweiligen Systemschiene (dev, test, prod) oder die Unterteilung der Rollen in Einzelrollen, Sammelrollen und Rollen für technische Benutzer.

Zum Thema Entwicklungsbereiche im Zusammenhang mit den SAP HANA extended application services, advanced model (XSA) wird auf die Empfehlungen von SAP verwiesen.

1.4 Aufbau des Transports

Ein Transportsystem auf Basis von CTS oder Import/Export ist möglich. Wenn keine CTS-Landschaft vorhanden ist oder unabhängig davon transportiert werden soll, kann für den Transport der in HANA bereits als XS-Applikation enthaltene SAP HANA application lifecycle manager (HALM) genutzt werden. Dieser bietet eine Transporthistorie sowie eine einfache Bedienbarkeit über die Web-Oberfläche und kann unabhängig vom Einsatzszenario der HANA-Instanz verwendet werden.

Bei der Entwicklung und dem anschließenden Transport von HANA-Rollen unterscheidet sich das Vorgehen nicht von anderen Entwicklungen. Demnach werden auch HANA-Rollen im Entwicklungssystem zusammengestellt und von dort zunächst in Test- und Q/A-Systeme transportiert, von wo aus sie letztlich in das/die Produktivsystem/-e gelangen.

Der Berechtigungsumfang sollte über die verschiedenen Systeme der Transportschiene abnehmen, sprich die meisten Berechtigungen sind im Entwicklungssystem vorhanden, im Produktivsystem die wenigsten. Entsprechend werden von einem System in das nächste immer nur die Rollen transportiert, die im Zielsystem zwingend notwendig sind.

Entwicklerrollen werden nicht in Test- oder Produktivsysteme transportiert. Rollen für grundlegende Funktionalitäten, wie beispielsweise Zugriffe auf _SYS_BIC-, _SYS_BI-Schemata oder die Verwendung von JDBC/ODBC-Schnittstellen, können dagegen auf der gesamten Systemschiene identisch transportiert und verwendet werden, um den Bau von redundanten Rollen zu vermeiden.

Systeme	Rollenumfang		
	Entwicklung	Test | Q/A	Produktion
SID1 (Dev)	X	X	X
SID2 (Test)		X	X
SID3 (Prod)			X

Tabelle 1: Umgebungsbezogene Verwendung von Rollen

Quelle: Eigene Darstellung

Bei der Verwendung von Rollen, die wiederum auf andere Rollen referenzieren (Sammelrollen), ist darauf zu achten, dass die Referenzen (Einzelrollen) zuerst transportiert werden müssen. Es empfiehlt sich daher, Einzel- und Sammelrollen in unterschiedliche Pakete aufzuteilen und diese nacheinander zu transportieren. Das Konzept von Einzel- und Sammelrollen im Zusammenhang mit HANA ist an die ABAP-Welt angelehnt, aber davon unabhängig zu betrachten. Da es sich dort als nützlich erwiesen hat und ein solches Konzept in HANA nicht existiert, kann es in HANA so umgesetzt werden, dass eine Einzelrolle eine Rolle beschreibt, die nur Berechtigungen beinhaltet, während eine Sammelrolle eine Rolle beschreibt, die auch (oder nur) andere Rollen beinhaltet.

Gibt es Abhängigkeiten der erstellten Rollen von Entwicklungsobjekten in anderen Delivery-Units, sind diese entsprechend immer vor den Rollen zu transportieren.

1.5 Namenskonvention

Eine durchdachte und nachhaltige Namenskonvention spielt eine ähnlich wichtige Rolle für SAP-HANA-Rollen wie für die in der ABAP-Welt. Es empfiehlt sich, diese schriftlich festzuhalten und als Pflichtlektüre allen Mitarbeitern der Rollenadministration an die Hand zu geben. Nur dadurch kann sichergestellt werden, dass unabhängig von der bearbeitenden Person die Rollennamen einheitlich verwendet werden.

Als generelle Faustregel kann für die Namenskonvention von Rollen Folgendes festgehalten werden: Sie muss kurz, aussagekräftig und eindeutig sein. Die Befolgung dieser Regel reduziert nicht nur die administrativen Aufwände, sondern erleichtert auch um einiges die Rollen- und Berechtigungsanalysen im System.

Bevor man auf Vorschläge und Best Practices der Namenskonvention eingeht, sei hier ein kurzer Abriss einiger technischer Besonderheiten der SAP-HANA-Rollen gegeben, die man bei der Namensgebung berücksichtigen muss.

Das einzig mögliche Sonderzeichen im Rollennamen ist „_“. Die oft verwendeten Sonderzeichen „/“ und „:“ für die Kennzeichnung der Namensräume und der Rollentypen finden hier keine Anwendung.

Als Trennzeichen im Rollennamen lassen sich somit keine Hyphens, sondern nur Unterstriche und Camel-Cases verwenden.

Rollennamen dürfen nur mit Buchstaben beginnen und dürfen keine Zahlen enthalten.

Die einzigen „:“ finden sich bei Designzeitrollen wieder, und sie dienen der Abtrennung der Paketpfade vom Objektnamen, z. B. sap.hana.ide.roles::Developer.

Die mögliche Zeichenlänge der Rollen reicht weit über die aus dem NetWeaver ABAP bekannten 30 Zeichen hinaus[1], sollte allerdings mit Bedacht verwendet werden (siehe Faustregeln der Namenskonvention).

Anders als in der ABAP-Welt ist in SAP HANA das Konzept von Einzel- und Sammelrollen aufgeweicht worden. Eine Rollenvererbung kann beliebig oft vorgenommen werden, und jede Rolle kann Privilegien enthalten. Folglich kann eine traditionelle Einzelrolle auch selbst weitere Rollen vererben. Es empfiehlt sich jedoch, für eine bessere Übersichtlichkeit und einen geringeren administrativen Aufwand eine Arbeitsplatzrolle mit sprechendem Namen zu definieren, die weitere Unterrollen und Berechtigungen enthält. Dennoch kann ein Konzept aus Sammel- und Einzelrollen zur Wiederverwendbarkeit von Rollen sinnvoll sein.

Der vollständig qualifizierte Name der Designzeitrollen lässt sich gut zur Strukturierung nutzen. Mithilfe der Paketstruktur kann man schon im Vorfeld die Rollen nach Typen (Sammel- oder Einzelrolle), System und Aufgabenbereich ordnen.

Laufzeitrollen lassen sich von Designzeitrollen leicht über den vollständig qualifizierten Namen auseinanderhalten, da Laufzeitrollen im Normalfall keinen Paketfaden besitzen.

In SAP HANA existieren keine abgeleiteten Rollen; diese bedürfen daher keiner Berücksichtigung in der Namenskonvention.

Tipp:

Die zeitgleiche Nutzung von Klein- oder Großbuchstaben im Rollennamen lässt sich nur bei der Verwendung von Camel-Cases für die Wörtertrennung hinreichend

[1] In SAP HANA kann der vollständig qualifizierte Name von Datenbankobjekten bis zu 127 Zeichen lang sein. Siehe Feld MAXIMUM_LENGTH_OF_IDENTIFIER in der Tabelle SYS.M_SYSTEM_LIMITATIONS.

begründen, siehe die SAP-HANA-Standard-Designzeitrollen wie „sap.hana.xs.admin.roles::JobAdministrator“. Die Ursache hierfür liegt in der Case-Sensitivity von SQL-Queries und bei der Verkettung von Rollen. Um aufwendigere SQL-Abfragen mit Berücksichtigung der Case-Sensitivity zu vermeiden, wird empfohlen, nur eine der beiden Schreibweisen zu verwenden, z. B. „BASIS_ADMINISTRATOR“ oder „basis_administrator“.

Anders als beim Rollennamen sollte bei der Benennung der Pakete grundsätzlich die Kleinschreibung verwendet werden.

Aus den eben genannten Punkten lässt sich leicht schlussfolgern, dass die bisherige Namenskonvention aus der ABAP-Welt nicht ohne weiteres in SAP HANA zu übertragen ist. Der wohl markanteste Unterschied besteht in dem Präfix (Paketstruktur) der Designzeitrollen, das in die Namenskonvention einbezogen werden kann. Auf dieser Grundlage sind hier zwei unterschiedliche Ansätze dargestellt: einmal mit Berücksichtigung der Paketstruktur, hier als kurze Namenskonvention bezeichnet, und einmal ohne, als lange Namenskonvention. In beiden Fällen wird die schriftliche Dokumentation der Paketstruktur ausdrücklich empfohlen.

1.5.1 Kurze Namenskonvention

In diesem Ansatz spielt die Paketstruktur eine übergeordnete Rolle, da hier die Informationen zu Systemumgebung, Aufgabenfeld und Rollentyp bereits mitgeliefert werden und in dem expliziten Rollennamen nicht weiter behandelt werden müssen.

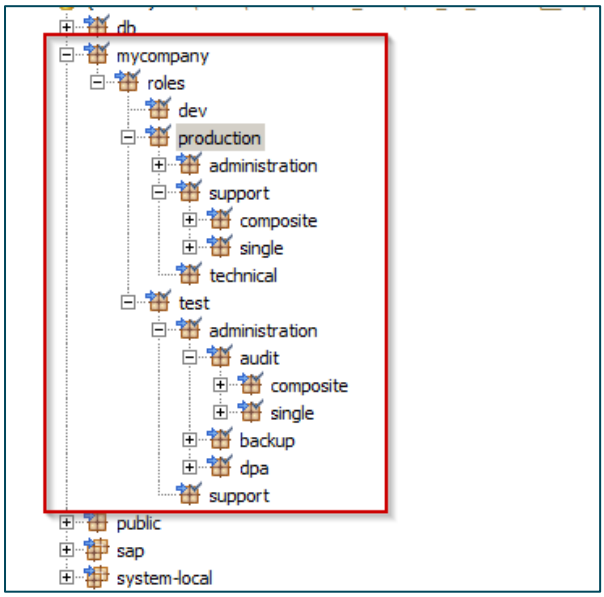


Abbildung 1: Paketstruktur für eine kurze Namenskonvention

Quelle: Eigene Darstellung

Hier unterscheiden wir Pakete für Produktions-, Test- und Entwicklungsumgebung. Eine Ebene tiefer in der Pakethierarchie werden die Aufgabenfelder und noch eine Ebene tiefer werden die Rollentypen angegeben.

Nachdem die Struktur angegeben wurde, können die Rollen wie folgt benannt werden.

Sammel-/Arbeitsplatzrollen:

- DEVELOPER (Entwickler)
- ANALYZER (Entwickler/Support-Mitarbeiter)
- BASIS_ADMIN (Basis-/Datenbankadministrator)
- ROLE_ADMIN (Rollenadministrator zur Anlage/Pflege der Berechtigungen)
- PROV_ADMIN (Datenbereitstellungsadministrator für Systemanbindungen über SDA)
- AUDIT_ADMIN (Compliance-Administrator)

Einzelrollen:

- Catalog: <*Berechtigung*>_CATALOG_<*Arbeitsplatz*>[_EXT]
  Beispiel: D_CATALOG_SYSTEMADMIN
- Content: <*Berechtigung*>_CONTENT_PCK_<*Paketname*>[_EXT]
  Beispiel: E_CONTENT_PCK_ROOT

In den ersten zwei Positionen der Einzelrollen wird die Aktivität angegeben: „D_“ für Display oder „E_“ für Edit. Das optionale Suffix „_EXT“ wird für Einzelrollen verwendet, die mit identischem Namen in mehreren Systemen vorkommen.

Beispiel:

Auf dem Produktivsystem gibt es die Rolle E_CONTENT_PCK_<*Paketname*>. Diese ist jedoch nur sehr wenig ausgeprägt. Die Rolle wird zudem auf dem Entwicklungssystem mit erweiterter Ausprägung benötigt. So kann die Rolle unter dem Namen E_CONTENT_PCK_<*Paketname*>_EXT auf dem Entwicklungssystem angelegt werden. Der entsprechende Arbeitsplatz auf dem Entwicklungssystem würde demnach dann beide Rollen erhalten: E_CONTENT_PCK_<*Paketname*> und E_CONTENT_PCK_<*Paketname*>_EXT.

Weiterhin sind Laufzeiteinzelrollen mit dem Präfix „RUNTIME“ zu versehen, wie das folgende Beispiel verdeutlicht:

- RUNTIME_D_DEBUGGING (Debugging)
- RUNTIME_E_DATAPROVISIONING (Data-Provisioning)

1.5.2 Lange Namenskonvention

Bei der langen Namenskonvention spielt die Pakethierarchie eine untergeordnete Rolle, und sie dient lediglich der grundsätzlichen Strukturierung der Rollen, die ihr Deployment in den Folgesystemen erlaubt. Die zusätzliche Unterteilung in composite („sammel“) bzw. single („einzel“) soll eine bessere Übersicht über die Rollen gewährleisten, hat aber keine Auswirkungen auf die Namenskonvention.

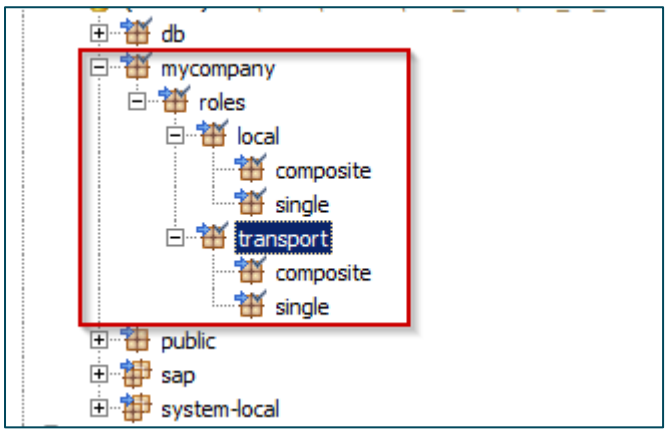


Abbildung 2: Paketstruktur für eine lange Namenskonvention

Quelle: Eigene Darstellung

Die lange Namenskonvention umfasst unterschiedliche Bestandteile der Rolle:

In Position 1-4 ist die Systemumgebung angegeben, für die die Rolle bestimmt ist. Die Namensgebung der Rollen bestimmt auch ihre Verwendung. Somit sind DEV/UAT[2]-Einzel- und -Sammelrollen nur in den dafür bestimmten Umgebungen zu nutzen. Eine Abweichung von dieser Regel bilden die Rollen für Produktion. Die PRD-Sammelrollen können sowohl in Produktion wie auch in der Testumgebung zum Einsatz kommen, während die PRD-Einzelrollen in allen Umgebungen zugeordnet werden dürfen. Den Grund für diese Herangehensweise bilden die Wiederverwendung und die Vermeidung redundanter Rollen. Demnach sollen Rollen für den Zugriff auf das _SYS_BIC-, _SYS_BI-Schema oder für die Verwendung der JDBC/ODBC-Schnittstelle in Rollen unterschiedlicher Umgebung verwendet werden, ohne sie umgebungsspezifisch neu zu gestalten.

[2] Das Kürzel UAT wird für alle Testumgebungen verwendet.

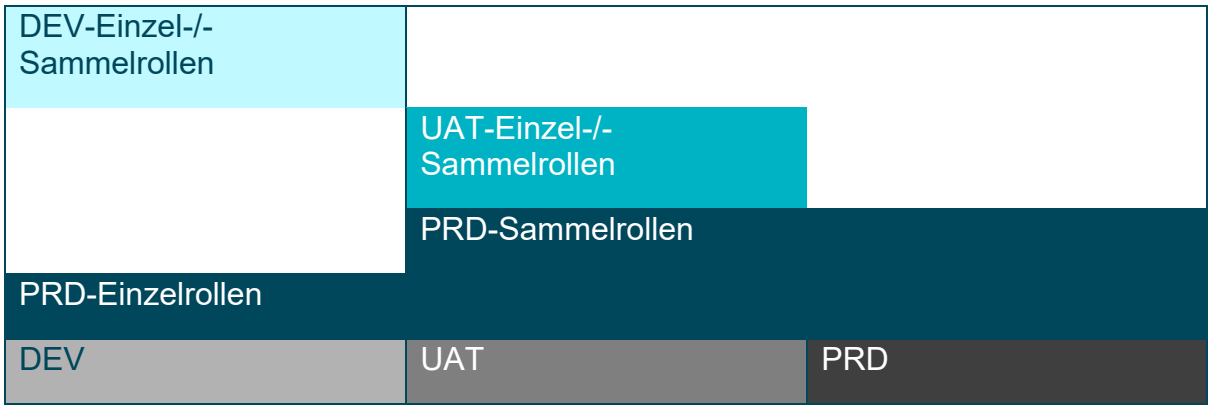


Tabelle 2: Kombination von Einzel- und Sammelrollen

Quelle: Eigene Darstellung

Position 5-6 kennzeichnet die Art der Rolle. Hier sind alle Rollen Sammelrollen – mit Ausnahme der _R_-Rolle – und müssen daher in dem Paket composite erstellt werden. Entsprechend sind die _R_-Rollen in dem Paket single zu erstellen. Sammelrollen dienen lediglich als Hülle für die Einzelrollen und ihnen ist kein Privileg zugeordnet.

Das Modul oder auch Applikationskürzel, für das die Rollen gültig sind, ist in den Positionen 7–10 zu definieren. Eine Eigenart bildet hier die Kennzeichnung US__. Hiermit sind Rollen gemeint, die universell, also über alle Systemumgebungen hinweg, verteilt werden. Solche Rollen wären i. d. R. Rollen für Drittanbieter-Tools.

Die Aktivitätseinstufung der Rollen findet in Position 1112 statt. Die Einteilung erfolgt hier in Lese- und Änderungsrollen.

Position	Inhalt	Beschreibung
1-4	**DEV_** = Role for development **UAT_** = Role for test system **PRD_** = Role for production	Systemumgebung
5-6	**A_** = Administrationsrolle **R_** = Einzelrolle **T_** = Technische User-Rolle **E_** = Notfallrolle **N_** = Business-Rolle	Rollentyp
7-9	*<2 Zeichen, z. B. FI>_*	Modul
10-11	**R_** = Read **M_** = Maintain	Aktivität
12-30	Freitext ROLE_ADMIN BASIS_ADMIN	Anwendungsfall

Tabelle 3: Namenskonvention

Quelle: Eigene Darstellung

Beispiel:

- PRD_A_HR_M_ROLE_ADMIN (Sammelrolle für Rollenadministration in Produktion)
- PRD_R_HR_R_ROLE_ADMIN (Einzelrolle für Rollenadministration mit Leserechten)
- UAT_N_FI_M_TESTER (Sammelrolle für Tester in der Testumgebung)

Eine leicht verkürzte Version dieser Namenskonvention mit ausschließlicher Kleinschreibung kann wie folgt aussehen:

- Die erste Position kennzeichnet den Rollentyp. „s“ für Einzelrolle sowie „c“ für Sammelrolle.
- Ohne Trennzeichen wird in den folgenden Positionen der Bezeichner aufgeführt.
- Nach dem Trennkennzeichen „_“ wird der Anwendungsfall festgehalten, und in der letzten Position, auch unter Verwendung des Trennkennzeichens, werden die möglichen Aktivitäten benannt.

Position	Inhalt	Beschreibung
1	**s** = Einzelrolle **c** = Sammelrolle	Rollentyp
2 - n	**basis_** = Basis-Administrationsrolle	Aufgabenbereich
	useradmin_ = Benutzeradministration	Anwendungsfall
	a = alle Berechtigungen **r** = Lesen **w** = Schreiben **x** = Ausführen	Aktivität

Tabelle 4: Verkürzte Namenskonvention

Quelle: Eigene Darstellung

Beispiel:

sbasis_useradmin_a

2 Berechtigungsebenen in der Administration

In einem Berechtigungskonzept findet in der Regel ein Ausgleich unterschiedlicher Anforderungen statt. Während die Administration gerne unbeschränkte Rechte (root/SAP_ALL) hätte, stehen dem Sicherheits- und Compliance-Interessen entgegen.

Das daraus resultierende „Minimalitätsprinzip“ und die Trennung von Verantwortlichkeiten bzw. Funktionen (Segregation of Duties – SoD) umzusetzen, ist in der Praxis immer wieder eine Herausforderung.

Für das allgemeine Administrations- und Tagesgeschäft empfiehlt es sich daher, unterschiedliche Berechtigungsebenen bzw. Kritikalitätsstufen und Prozesse/Workflows für die Vergabe von bestimmten Berechtigungen zu definieren. Dies gilt sowohl im Hinblick auf HANA-Rollen und -Privilegien (Autorisierung) als auch im Hinblick auf HANA-Benutzergruppen (Benutzerverwaltung), welche in einem späteren Kapitel detaillierter betrachtet werden.

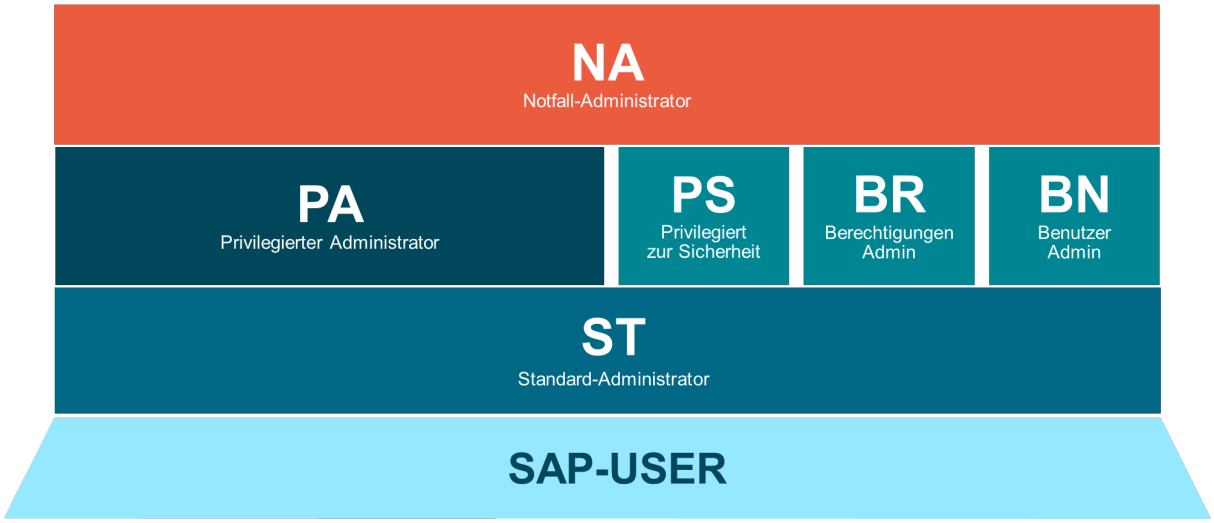


Abbildung 3: Berechtigungsebenen der Administration

Quelle: Eigene Darstellung

Diese Berechtigungsebenen sollten als klar definierte Stufen nach unterschiedlicher Kritikalität der Berechtigungen eingeteilt werden. Eine mögliche Einteilung solcher Ebenen, geordnet nach aufsteigender Kritikalität, sähe beispielsweise wie folgt aus:

- Tagesgeschäft Entwickler und ggf. Endanwender
- Tagesgeschäft Administratoren
- Besondere Berechtigungen im Einzelfall
- Notfälle

2.1 Definition der Kritikalität

Die Kritikalität einer Berechtigung kann nach den folgenden Kriterien eingestuft werden:

- wie sie durch die Kunden (Fachbereich, Revision), die IT-Sicherheit oder durch die Verantwortlichen für betroffene „Organisationseinheiten“ vorgegeben wird
- ob sie Berechtigungsobjekte enthält, die von Aktivitäten angefordert werden, die der Funktionstrennung unterliegen (SoD – Konflikte)

- ob sie besonders schutzbedürftige Objekte betrifft
- ob sie nach allgemeiner Praxis als kritisch bezeichnet wird, z. B. in einschlägigen Empfehlungen des BSI oder in Leitfäden von Prüfungsorganisationen, weil sie Aktivitäten ermöglichen, die die Schutzziele verletzen können oder zur Erlangung von Berechtigungen zu solchen Aktivitäten dienen.

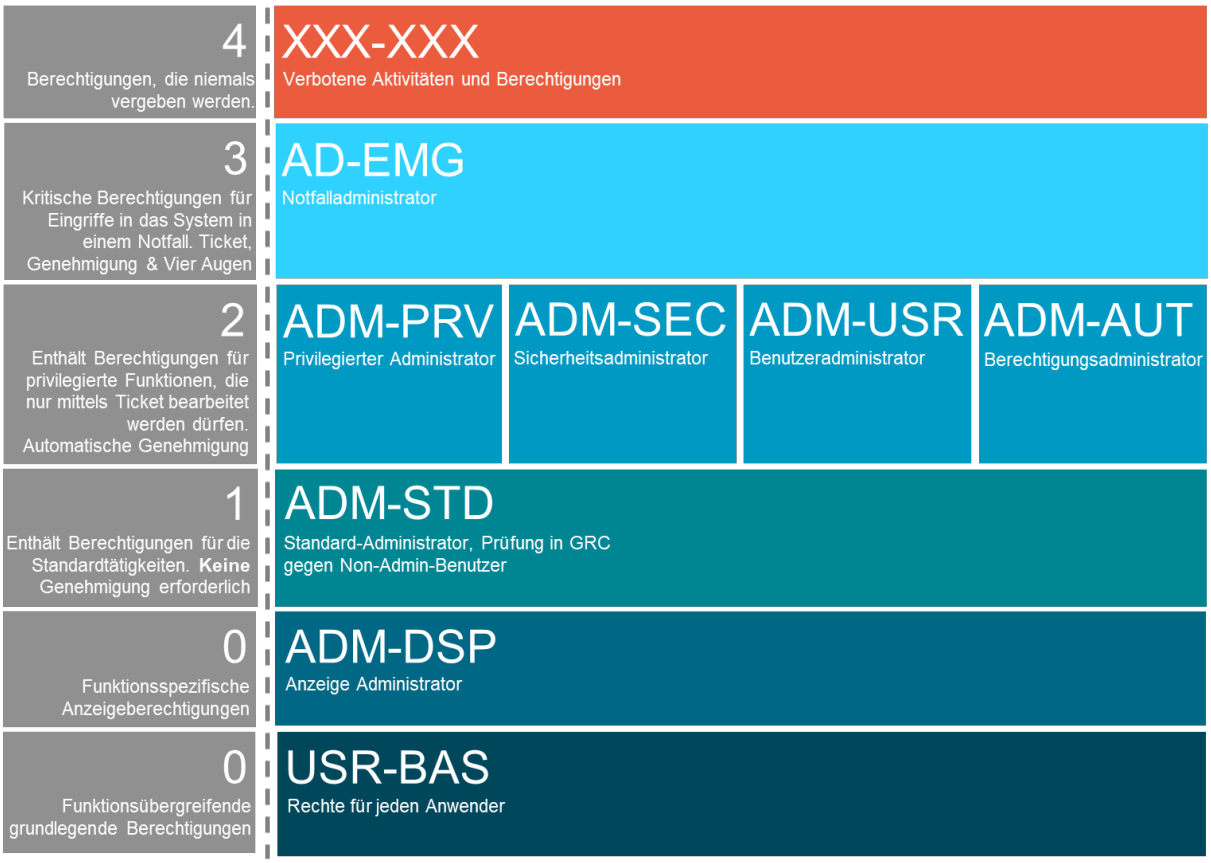


Abbildung 4: Kritikalitätsstufen und Rollen

Quelle: Eigene Darstellung

2.1.1 Ebene 0 Unkritische Berechtigungen

Eine Berechtigung gilt als unkritisch in den produktiven Systemen, wenn sie

- nur Lese- bzw. Anzeigerechte vergibt
- Änderungen und Anpassungen an einem System erlaubt, die aber die Verfügbarkeit und den Betriebsablauf nicht erheblich beeinträchtigen können
- keine Änderungen und Anpassungen an einem System erlaubt, die die Sicherheit des Systems (Integrität, Vertraulichkeit, Authentizität) gefährden
- nicht zur Änderung von schutzbedürftigen Objekten berechtigt

2.1.2 Ebene 1 Niedrige Kritikalität

Eine Berechtigung gilt als niedrigkritisch in den produktiven Systemen, wenn sie

- Änderungen und Anpassungen an einem System erlaubt, die die Verfügbarkeit und den Betriebsablauf beeinträchtigen können
- keine Änderungen und Anpassungen an einem System erlaubt, die die Sicherheit des Systems (Integrität, Vertraulichkeit, Authentizität) gefährden können
- nicht zur Änderung von schutzbedürftigen Objekten berechtigt

2.1.3 Ebene 2 Mittlere Kritikalität

Eine Berechtigung gilt als mittelkritisch in den produktiven Systemen, wenn sie

- Änderungen und Anpassungen an einem System erlaubt, die die Verfügbarkeit des Systems oder den Betriebsablauf erheblich beeinträchtigen können
- Änderungen und Anpassungen an einem System erlaubt, die schutzbedürftige Objekte des Systems unmittelbar verändern

Ab dieser Kritikalitätsstufe besteht ein erhöhtes Risiko, dass die Schutzziele Integrität und Vertraulichkeit zum System verletzt werden und ein Schaden für das Unternehmen verursacht wird. Daher müssen hier die Regeln zur Funktionstrennung (SoD) eingehalten werden!

2.1.4 Ebene 3 Hohe Kritikalität

Eine Berechtigung gilt als hochkritisch in den produktiven Systemen, wenn sie

- Änderungen und Anpassungen an einem System erlaubt, die die Verfügbarkeit des Systems oder den Betriebsablauf erheblich beeinträchtigen können
- Änderungen und Anpassungen an einem System erlaubt, die die Sicherheit des Systems (Integrität, Vertraulichkeit, Authentizität) gefährden können
- erlaubt, die Systemkontrollen außer Kraft zu setzen

Das Risiko mit derartigen Berechtigungen ist somit hoch, dass alle Schutzziele zum System gravierend verletzt werden und ein Schaden für das Unternehmen verursacht wird. Solche Berechtigungen sollten nur in Ausnahmesituationen bzw. Notfällen zur Anwendung kommen.

2.1.5 Ebene 4 Kritische Berechtigungen

Eine Berechtigung kann als kritisch eingestuft werden, wenn sie ein weitreichendes Risiko für die Schutzziele Integrität und Vertraulichkeit zum System darstellt. Eine als kritisch eingestufte Berechtigung sollte in der Praxis überhaupt nicht vergeben werden.

2.2 Die Berechtigungsebenen in der Praxis

Im Folgenden werden die oben angesprochenen möglichen Berechtigungsebenen erläutert und zu den genannten Kritikalitätsstufen für Berechtigungen in Beziehung gesetzt.

2.2.1 Ebene 0, 1: Tagesgeschäft Entwickler und ggf. Endanwender

Die erste Ebene ist relativ selbsterklärend und umfasst Berechtigungen, welche im normalen Tagesgeschäft regelmäßig benötigt werden. Die Vergabe dieser Berechtigungen erfolgt auf Basis eines einheitlichen Workflows durch die Rollenadministration. Die Berechtigungen liegen je nach konkreter Tätigkeit bzw. Rolle in den Stufen unkritisch bis maximal niedrigkritisch.

2.2.2 Ebene 2: Tagesgeschäft Administratoren

Auch die zweite Ebene umfasst Berechtigungen zum normalen Tagesgeschäft, allerdings auf der Administrationsebene. Die Vergabe dieser Berechtigungen erfolgt ebenfalls auf Basis eines einheitlichen Workflows durch die Rollenadministration. Dabei steht weiterhin das Prinzip der Funktionstrennung im Vordergrund. So sollten etwa Rollen- und Benutzeradministration getrennt werden und derart umfangreiche Berechtigungen nur dort erteilt werden, wo sie wirklich benötigt werden. Die Berechtigungen dafür erstrecken sich bis auf die Stufe der mittleren Kritikalität.

2.2.3 Ebene 3: besondere Berechtigungen im Einzelfall

Die dritte Ebene umfasst besondere Berechtigungen, welche üblicherweise im Tagesgeschäft nicht notwendig sind. Dies können beispielsweise außergewöhnliche Tests oder Analysen sein, welche noch keinen Notfall darstellen, oder aber die temporäre Notwendigkeit zusätzlicher Administrationsberechtigungen. Für Analysen außerhalb des Entwicklungssystems kann in dem Fall ein spezieller Analysebenutzer eingerichtet werden, welcher im begründeten Bedarfsfall freigeschaltet wird; weitergehende Administrationsberechtigungen können in Abstimmung mit der Rollenadministration vergeben werden. Die Vergabe solcher Berechtigungen wird strikter behandelt, sollte nur temporär erfolgen und nachvollziehbar dokumentiert werden. Die dafür notwendigen Berechtigungen können mitunter als mittel- bis hochkritisch eingestuft werden.

2.2.4 Ebene 4: Notfälle

Die letzte und kritischste Ebene umfasst Notfallsituationen. Darunter fallen unvorhergesehene Situationen, welche oftmals zeitkritisch sind und weitreichende Berechtigungen erfordern. Der BSI-Standard 100-4 für Notfallmanagement definiert den Notfall als ein Ereignis, wodurch Prozesse oder Ressourcen einer Institution oder eines Unternehmens längerfristig ausfallen und dadurch ein hoher oder sehr hoher Schaden verursacht wird. Zugleich weist das Rahmenwerk auf die Bedeutung einer eigenen Definition hin, wann ein Notfall oder eine Störung vorliegt, denn nicht alles, was auf den ersten Blick als Notfall erscheint, ist auch einer.[3]

[3] BSI, BSI-Standard 100-4 (2008), S. 5.

Je nach eigener Definition von Notfällen und dem Umgang mit diesen kann dies beispielsweise die Aktivierung des SYSTEM-Benutzers über einen definierten Workflow oder den Einsatz spezieller Firefighter-Benutzer bedeuten. In jedem Fall muss für derart kritische Berechtigungen genau festgelegt werden, wer diese in welchen Situationen anfordern darf, siehe dazu das Kapitel „Notfalladministration“. Die Nutzung darf nur temporär erfolgen und muss nachvollziehbar dokumentiert werden. Diese Berechtigungen sind in den meisten Fällen als hochkritisch kategorisiert.

3 Notfalladministration

Das BSI veröffentlicht jährlich das IT-Grundschutzkompendium, in dem konkrete Anforderungen an die Absicherung eines SAP-Systems abgefasst sind. Diese wurden im sogenannten Systembaustein APP.4.2 SAP-ERP-System zusammengefasst und beinhalten u. a. die Erstellung eines Notfallkonzepts und das Einrichten eines Notfallbenutzers. Obwohl in der Einleitung des ERP-Systembausteins eine Abgrenzung zu SAP HANA vorgenommen wird,[4] ist es dennoch ausdrücklich empfohlen, HANA als Kernkomponente des ERP-Systems in das Notfallkonzept mit einzubeziehen.

Das Notfallkonzept wird an dieser Stelle als IT-Service-Kontinuitätsmanagement nach ITIL verstanden. Es soll im Einklang mit dem Business-Continuity-Management die Aufrechthaltung des IT-Betriebs nach Notfällen sicherstellen. Nach dem IT-Grundschutz-Kompendium umfasst das Notfallkonzept für ein SAP-ERP-System drei Elemente:

1. die Feststellung von und Reaktion auf Zwischenfälle als eine Art Notfallvorsorgekonzept,
2. das Backup- und Wiederherstellungskonzept sowie
3. die Notfall-Administration.[5]

Für den Leitfaden ist der letzte Teil relevant, da unter der Notfalladministration folgende Themen zusammengefasst werden können:

1. das Notfallberechtigungskonzept,
2. die Notfallbenutzer sowie
3. die Kontrolle und Protokollierung der Nutzung der Notfallrechte.

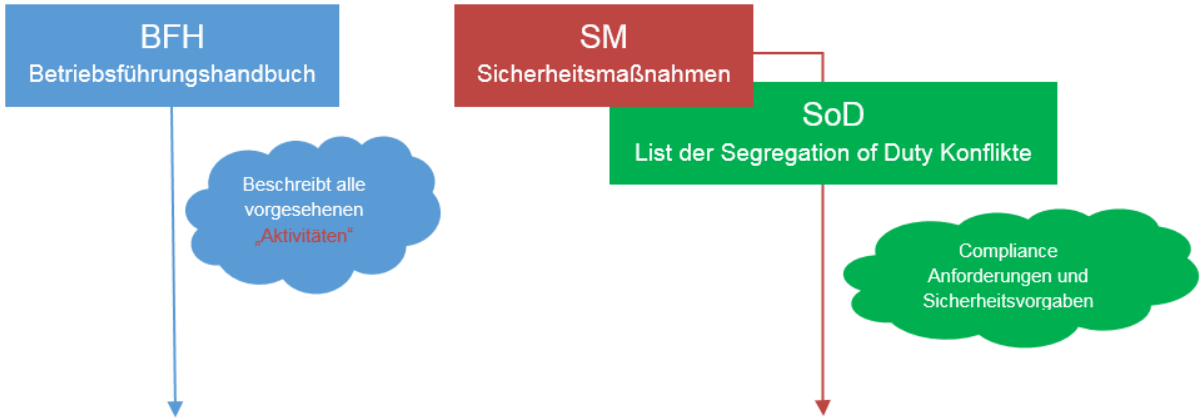
3.1 Kritische Berechtigungen

Grundlage des Notfallberechtigungskonzeptes ist die Identifikation der kritischen Berechtigungen, die über den pragmatischen Ansatz der Zusammenführung der Kritikalitätsstufen und der korrespondierenden Berechtigungsebenen erreicht werden

[4] BSI, IT-Grundschutz-Kompendium (2020), APP.4: Business-Anwendungen, S. 1.
[5] BSI, IT-Grundschutz-Kompendium (2020), APP.4: Business-Anwendungen, S. 6.

kann. Hierbei entsteht eine Matrix, die im Wesentlichen zwei Quellen von Anforderungen betrachtet: die (betrieblichen) Aktivitäten, wie sie idealerweise im Betriebshandbuch oder Betriebsverfahrenshandbuch beschrieben sind, und die Compliance- oder Sicherheitsanforderungen.

Zwischen Aktivität (Beispiel: Backup einspielen) und technischer Berechtigung (bzw. Rolle) lässt sich in den meisten Fällen eine eindeutige Zuordnung festhalten. Die Einstufung der Kritikalität ist nicht immer ganz einfach, wird aber durch die Definition von Kritikalitätsstufen und Berechtigungsebenen erleichtert. Hier ist nur die im vorherigen Kapitel beschriebene dritte Kritikalitätsstufe von Belang.



Aktivität	BFH#	Kritikalitäts-Stufe	Berechtigung	Rolle	System
Systemeinstellungen ändern	BFH-B-HANA-nn-nn	2	INIFILE ADMIN	ADM-PRV	PROD
Audit-Einstellungen ändern	BFH-B-HANA-nn-nn	3	AUDIT ADMIN	ADM-EMG	PROD
Objektstrukturen ändern	BFH-B-HANA-nn-nn	3	DATA ADMIN	ADM-EMG	PROD
Trace Konfigurieren	BFH-B-HANA-nn-nn	2	TRACE ADMIN	AMD-PRV	PROD

Abbildung 5: Identifikation der kritischen Berechtigungen

Quelle: Eigene Darstellung

Hat man erst die Berechtigungen identifiziert, können diese in eine oder mehrere Rollen überführt werden. Das kann man davon abhängig machen, ob die Berechtigungsebene der Notfalladministration nur eine oder noch zusätzliche Gruppen umfassen soll. Eine Überlegung wäre, die Berechtigungen für die Business-Anwendung, die im Wesentlichen auf das benutzerdefinierte Schema und Repository abzielen, von den Datenbankadministrationstätigkeiten zu trennen. Der Grund hierfür ist die Wahrung der Funktionstrennungsrichtlinie. Zudem hat es sich bewährt, die Berechtigungen für die Auditadministration sowie die Rollen- und Benutzerpflege aus

der Notfalladministrationsrolle zu entfernen und sie in die Rollen der privilegierten Berechtigungsebenen einzubetten.

Abbildung 6: Notfalladministration und privilegierte Berechtigungsebenen

Quelle: Eigene Darstellung

Unabhängig davon, wie viele Rollen oder Gruppen für die Notfalladministration definiert werden, das Stellenprinzip muss zu jeder Zeit gewahrt bleiben. Eine mögliche Herausforderung kann sich hier aus den organisatorischen Gegebenheiten des Betriebs ergeben. Wenn für die gesamte SAP HANA-Datenbankadministration nur eine Funktionsgruppe zuständig ist, dann wird auch eine granulare Funktionstrennung schwieriger zu gestalten sein. Nichtsdestotrotz empfiehlt es sich, wenn möglich eine Berechtigungstrennung wie im obigen Beispiel zu implementieren.

3.2 Zugriff auf Notfallrechte

Der Zugriff auf die Notfallrechte kann über zwei Wege erfolgen: entweder durch einen Notfallbenutzer oder durch die individuelle Direktzuweisung der Notfallrollen.

3.2.1 Notfallbenutzer

Für das Notfallkonzept sieht das BSI die Erstellung von Benutzer-IDs für Notfallbenutzer vor.[6] Diese Benutzer werden die Notfallrolle bereits zugewiesen bekommen haben und diese soll unmittelbar genutzt werden. Für das Einloggen stehen die gängigen Authentifizierungsmechanismen von SAP HANA zu Verfügung. Entscheidet man sich für die Authentifizierung mittels Kennwort, dann sollte man daran denken, dieses nach jeder Verwendung neu zu setzen. Außerdem soll der Notfallbenutzer während der Inaktivitätsperiode gesperrt bleiben.

Wie viele Notfall-IDs im System im Endeffekt angelegt werden, hängt hauptsächlich davon ab, wie viele Notfallgruppen in Anwendung sind und wie viele parallele Verbindungen erlaubt sein sollen. Somit kann ihre Zahl von Fall zu Fall stark variieren, aber von einer zu hohen Zahl ist grundsätzlich abzuraten, da hoch privilegierte Benutzer als potenzielle Angriffsvektoren dienen.

[6] BSI, IT-Grundschutz-Kompendium (2020), APP.4: Business-Anwendungen, S. 7.

Es ist häufig der Fall, dass man auf den SYSTEM-Benutzer als Notfallbenutzer zurückgreift. SAP rät nicht davon ab[7] und es kann durchaus eine valide Lösung sein, wenn eine einfache Lösung bevorzugt wird. Der SYSTEM-Benutzer verfügt bereits über die notwendigen Berechtigungen, um SAP HANA zu administrieren, wenn auch mit gewissen Abstrichen, z. B. was die Applikationszugriffe betrifft. Sind darüber hinaus kundeneigene Schemas in Nutzung, dann müssen diese explizit berechtigt werden. Zugleich sollte man wegen der Berechtigungen des Benutzers auch hinsichtlich der Audit-, Rollen- und Benutzeradministration Vorsicht walten lassen.

Eine einfache Kopie des SYSTEM-Benutzers ist nicht möglich, wie es auch der Hinweis 2166489 verdeutlicht. Der Grund liegt in der Benutzerkopie-Funktion, die direkt zugewiesene Privilegien sowie die Katalogrollen nicht mitkopiert.

Eine Kopie des SYSTEM die sich dem Ideal der identischen Kopie nähert, würde die eigentliche Idee ad absurdum führen, denn dieser User wäre exakt gleich mächtig, es wäre also wenig gewonnen. Dennoch kann man durchaus versuchen, sich diesem Ziel zu nähern, wobei man zugleich potenzielle SOD-Konflikte ausschließt, also USER ADMIN, ROLE ADMIN und AUDIT ADMIN bewusst ausschließt. Als Grundlage bietet sich dann eine Analyse der tatsächlichen Privilegien des SYSTEM über den View SYS. GRANTED_PRIVILEGES (wobei man nach SYSTEMDB und Tenant unterscheiden muss). Beispielsweise:

```
SELECT
        "GRANTEE",
        "OBJECT_TYPE",
        "SCHEMA_NAME",
        "OBJECT_NAME",
        "PRIVILEGE",
        "IS_VALID"
FROM "SYS"."GRANTED_PRIVILEGES" where grantee = 'SYSTEM' and is_valid = 'TRUE';
```

Die daraus resultierende Rolle ist schon sehr mächtig und ermöglicht es die Freischaltung des SYSTEM als quasi ultima ratio deutlich hinaus zu schieben. [8]

Für die Erstellung muss der SYSTEM-User selbst genutzt werden, damit es keine Probleme aufgrund von fehlenden Privilegien gibt.

3.2.2 Rollenbasiert

Die Direktzuweisung der Notfallrollen ist eine valide Alternative zum ID-basierten Vorgehen. In diesem Fall werden die zuvor erstellten kritischen Rollen dem

[7] SAP HANA Security Guide, S. 89.
[8] https://www.dsag.de/beitraege/admin-user-mit-system-rollen-und-berechtigungen.

personalisierten Benutzer manuell oder automatisiert für die Dauer des Notfalls zugeordnet und anschließend wieder entfernt.

Der Vorteil liegt in der höheren Flexibilität, da bei der Änderung der Notfallgruppen keine IDs nachgezogen werden müssen. Lediglich das Stellenprinzip ist zu wahren. Die Flexibilität kommt allerdings mit einem erhöhten Aufwand für die Governance einher, weil das Logging benutzerspezifisch und aktiv angepasst werden muss.

Zudem ist sicherzustellen, dass mindestens für folgende Aktionen Policies definiert werden[9]:

- Benutzerpflege
- Pflege von Katalog- und HDI-Rollen
- Zuordnung von Rollen und Berechtigungen
- Pflege von Systemparametern
- Ausführung von DDL-Befehlen im Produktivsystem
- Konfiguration der Verschlüsselung
- Anschluss neuer Systeme zur Authentifizierung
- Installieren und Löschen von Lizenzen
- Pflege von Remote Sources
- Importieren und Aktivieren von Repository-Content
- Zugriff auf ERP-/S/4HANA-Daten
- Pflege von Tenant-Datenbanken (nur in der System-DB)
- Starten und Stoppen von Tenant-Datenbanken (nur in der System-DB)

3.3 Governance

Die Kritikalität der Notfallrechte und somit das gesteigerte Risiko für Datensicherheit, -verfügbarkeit und -integrität macht es notwendig, dass die Auflagen für die Nutzung der Notfallrechte recht hoch entfallen. Diese Auflagen umfassen:

- entsprechend dem Stellenprinzip die Berechtigung zu einer Notfallgruppe zugeordnet zu werden,
- die Bedingungen, unter welchen eine Aktivierung stattfinden darf,
- die Protokollierung sowie
- ein Ausweichplan, wenn automatisierte Teile des Prozesses versagen.

Unabhängig davon, welche Methode für die Zuordnung der Notfallrechte verwendet wird: Die Liste der Personen, welche für die Notfallgruppe(n) autorisiert sind, muss immer aktuell und verfügbar sein. Auch muss überwacht werden, ob ausschließlich die in der Liste geführten Benutzer sich Zugriff verschafft haben. Das kann man über

[9] https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.04/en-US/35eb4e567d53456088755b8131b7ed1d.html.

den SAP HANA Audit Log nachhalten, da unter den Feldern „APPLICATION_USER_NAME“ und „CLIENT_HOST“ der Endanwender und sein Client geloggt werden.

Um die Notfallrechte zu aktiveren, bedarf es eines gültigen Tickets (Major Incident oder Request for Change), in dem das Zielsystem, die Begründung sowie die benötigte Notfallgruppe und die ausführende Person spezifiziert sind. Gegebenenfalls kann auch die Dauer angegeben werden, was eher auf geplante Tätigkeiten zutrifft. Der Zugriff darf nur so lange gestattet sein, solange das referenzierte Ticket in Bearbeitung ist. Darüber hinaus ist es ratsam, ein zeitliches Limit von zwölf Stunden zu setzen, das greift, wenn das Ticket nicht binnen dieser Zeit geschlossen wird.

Die Freischaltung der Notfallrechte darf nur mittels Freigabe durch eine Vier-Augen-Kontrolle erfolgen. Es ist somit eine Genehmigung vom Manager on Duty oder vom Applikationsverantwortlichen einzuholen, der die Richtigkeit des Notfallzugriffs beurteilen soll. Die Genehmigung löst dann entweder die Rollenzuordnung zu dem Endbenutzer aus oder führt dazu, dass der Notfallbenutzer entsperrt und ein neues Kennwort vergeben wird.

Um die Revisionssicherheit sowie die Protokollierung der Aktivitäten und ihre Nachvollziehbarkeit zu gewährleisten, muss der Notfallbenutzer vollumfänglich auditiert werden. Auch müssen die für die Freischaltung notwendigen Daten aufbewahrt werden. Der Antragsteller, Genehmiger, eventuell die Notfallgruppe, Datum und Dauer der Nutzung sowie die Ticket-ID sind festzuhalten. Wegen der Eigenheit von SAP HANA, in der eine Audit-Policy nur eine Audit-Kategorie umfassen kann, ist es ratsam, die Kategorisierung zu umgehen, und das Loggen aller Tätigkeiten auszuwählen. Während beim dedizierten Notfallbenutzer die Auditierung rund um die Uhrzeit eingeschaltet bleiben kann, ist beim rollenbasierten Konzept die Protokollierung nur für die Dauer der Nutzung ratsam.

Folgende Policy kann für Notfallbenutzer definiert werden:

- Audited Action Status ALL
  (Protokollierung aller Aktionen; erfolgreiche und fehlgeschlagene)
- Audited Actions ALL ACTIONS
- Audited Objects *<keine Einschränkung>*
- Audited Users <Auflistung der Notfallbenutzer>

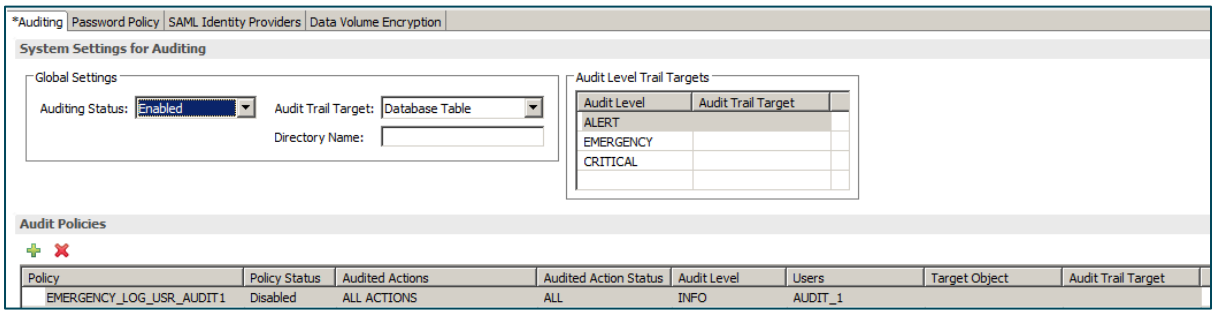


Abbildung 7: Audit Einstellungsmaske

Quelle: Eigene Darstellung

Nicht zuletzt muss das Notfallkonzept auch eine Ausweichlösung vorsehen, die den Prozess auch dann ermöglicht, wenn das für die Automatisierung vorgesehene System ausfällt. SAP bietet eine Tool-basierte Lösung mit dem Modul Emergency Access Management von GRC Access Control an. Das Tool ist ab der Version 10.1 mit SAP HANA kompatibel und es unterstützt sowohl das notfallbenutzerbasierte wie auch das rollenbasierte Notfallkonzept, inklusive der Möglichkeit für eine umfangreiche Protokollierung und einen Freigabeprozess. Nachteil der Lösung ist, dass die Funktionen auf SAP GRC zentralisiert sind. Ist das System nicht verfügbar, dann muss man auf einen manuellen Prozess ausweichen. Des Weiteren braucht man die User Access Management-Komponente für die Benutzerfreischaltung und Rollenzuweisung.

4 Abhängigkeiten zu DBA Cockpit

Das SAP NetWeaver-ABAP-System bietet für die Datenbankadministration und das Datenbankmonitoring ein plattformunabhängiges Tool an: das DBA Cockpit. Es wird über die Transaktion DBACOCKPIT aufgerufen und kann sowohl vom lokalen SAP-System als auch zentral über den Solution Manager genutzt werden.

Werden keine weiteren Schritte bei der Installation des SAP-Systems unternommen, so ist hinter dieser Transaktion die DEFAULT-Datenbankverbindung mit dem Schema-User (SAPABAP1/SAPJAVA1) des SAP-Systems verborgen.

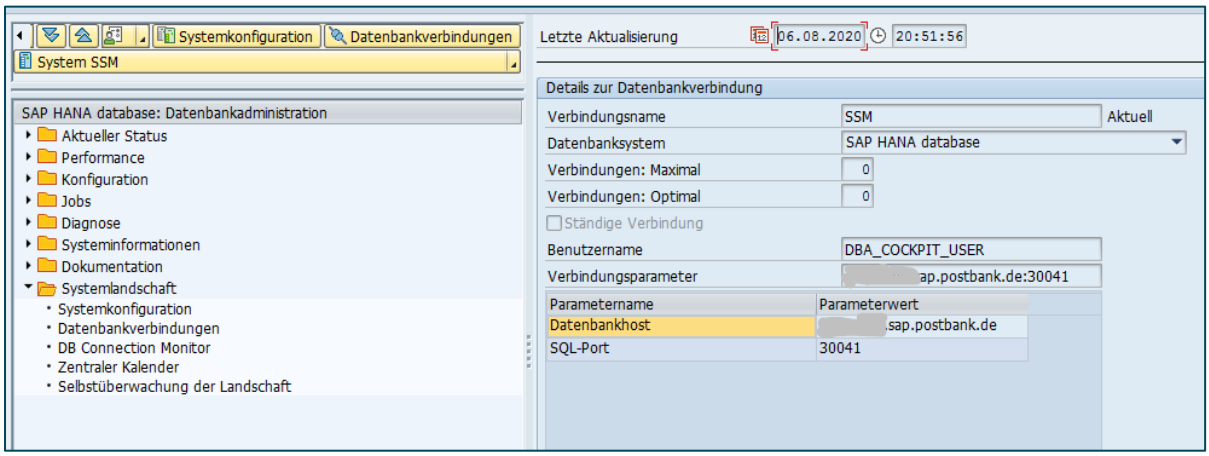


Abbildung 8: Default Datenbankverbindung

Quelle: Eigene Darstellung

Dieser Schema-User hat über die Rolle DBA_COCKPIT auch weitreichende Administrationsrechte auf der Datenbank.

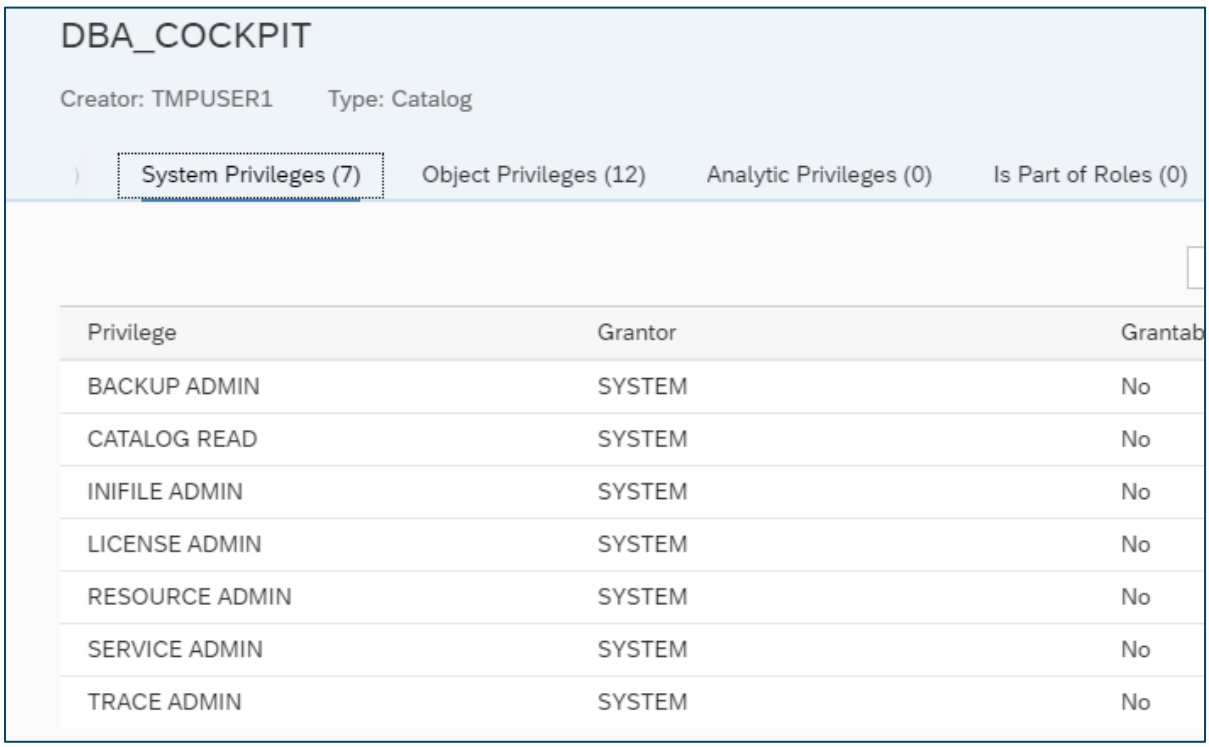


Abbildung 9: DBA_COCKPIT-Rolle

Quelle: Eigene Darstellung

Kritisch sind hier vor allem die Systemprivilegien ‚INIFILE ADMIN' und ‚BACKUP ADMIN'. Um zu verhindern, dass über PFCG-Rollen berechtigte NetWeaver-User im DBA Cockpit plötzlich solche Datenbankadministrationsrechte erhalten, kann folgendes Vorgehen gewählt werden.

Rolle DBA_COCKPIT_CUST_C

Anhand der Rolle DBA_COCKPIT wird eine eingeschränkte Kundenrolle erstellt. Hier fehlt vor allem das „INIFILE ADMIN“ und das Systemprivileg „BACKUP ADMIN“ wird durch „BACKUP OPERATOR“ ersetzt.

Technischer User (DBA_COCKPIT_USER)

Diesem technischen User wird die gerade beschriebene Rolle zugewiesen.

Datenbankverbindung <SID>

Wird über die Transaktion DBCO im SAP-System eine Datenbankverbindung hinterlegt, die im Namen (Feld: DB-Verbindung) die SAP-<*SID*> enthält.

Beim Aufruf des DBA Cockpit wird nun diese Verbindung statt der DEFAULT-Verbindung genutzt.[10]

5 SAP HANA-Support-Prozess

5.1 Die Rolle SAP_INTERNAL_HANA_SUPPORT

Der SAP-Support-Benutzer muss dediziert angelegt werden (siehe SAP-Hinweis **1747042)**.

Die Rolle SAP_INTERNAL_HANA_SUPPORT kann per Standard nur einmal zugeordnet werden, außerdem kann diese Laufzeitrolle nicht ohne weiteres in eine kundeneigene Repository-Rolle überführt werden, da die Rolle dem Benutzer SYS gehört. Die Rolle enthält Berechtigungen für den Lesezugriff auf alle Metadaten der Datenbank (System-Privileg CATALOG READ), auf den aktuellen Systemstatus, auf die Trace-Konfiguration und die Daten des Statistikservers (Schema _SYS_STATISTICS) sowie auf alle Systeminformationen aus dem SYS-Schema.

Die Leserechte auf das SYS-Schema sind nur dieser Rolle und nur dem SYSTEM-Benutzer gestattet, wobei der SYSTEM-Benutzer die Zugriffsrechte nicht weitervererben kann. Folglich ist man bei einem Zugriff auf Tabellen/Views wie die TOPOLOGY_INFORMATION_ auf eine der beiden Alternativen angewiesen. In solchen Fällen ist es sinnvoll, die Zuordnungsgrenze für die SAP_INTERNAL_HANA_SUPPORT-Rolle auf > 1 zu setzen, um den zusätzlichen Aufwand zu vermeiden, die Rolle dem SAP-Support-Benutzer zu entziehen und im Anschluss erneut zuordnen zu müssen.

Offensichtlich hat SAP an dieser Stelle spezielle Vorkehrungen getroffen, um eine allzu leichtfertige Vergabe dieser mächtigen Rolle zu verhindern. Auch wenn man aus pragmatischen Gründen vielleicht mehr als eine Nutzerkennung für den Support

[10] 1640741 – FAQ: „DB-User für das DBA Cockpit für SAP HANA“.
2411438 – HANA MDC: Der DBCON-Eintrag der lokalen DB wird überschrieben.

benötigen wird, sollte man hier so restriktiv wie möglich vorgehen. Mit dem Systemparameter internal_support_user_limit (Datei nameserver.ini [für Systemdatenbanken] bzw. indexserver.ini [für Tenant-Datenbanken]) kann die Anzahl der maximal möglichen Zuweisungen festgelegt werden. Wird die Rolle einem weiteren Benutzer zugeordnet, wird die Fehlermeldung „*SQL (456) – not allowed for this role: grant to more than the preconfigured number (1) of users at a time*“ ausgegeben.

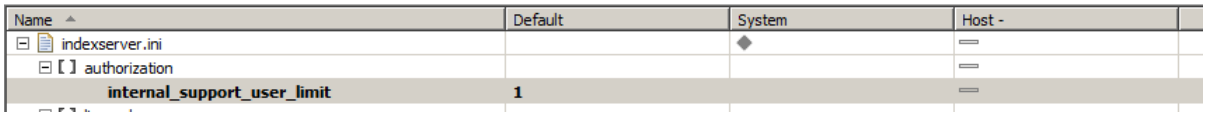


Abbildung 10: SAP_INTERNAL_HANA_SUPPORT-Rolle Zuweisungslimit

Quelle: Eigene Darstellung

Zusätzlich erzeugt die Zuordnung der Rolle automatisch einen Alarm (ID 63 Granting of SAP_INTERNAL_HANA_SUPPORT role); siehe SAP-Hinweis **2081857**.

Des Weiteren gilt für die Rolle:

- Es können keine weiteren Objektprivilegien zugeordnet werden.
- Die Rolle kann um Systemprivilegien erweitert werden.
- Die Rolle kann nicht in eine andere Rolle integriert werden.
- Bei jedem Upgrade wird die Rolle überschrieben.
- Sie kann nicht dem Benutzer SYSTEM zugeordnet werden (dieser verfügt bereits über die Berechtigungen aus der Rolle).

5.2 Vorgehensweise Support-Prozess

Bezüglich der benötigten Berechtigungen wird hier ein mehrstufiges Vorgehen empfohlen. Die SAP_INTERNAL_HANA_SUPPORT-Rolle ist inhaltlich nicht anzupassen. Weiterhin ist es ratsam, den Prozess für den SAP-Support-Zugriff zu definieren und zu standardisieren, wobei auch die Authentifizierungsmechanismen (ID/Kennwort, Zertifikate etc.) und die Gültigkeit der Verbindung anzugeben sind. Im Produktionsumfeld sollte die Verbindung nach 24 Stunden aufgelöst werden.

Es empfiehlt sich, den dedizierten SAP-Support-Benutzer (z. B. HANA_SUPPORT) dauerhaft im System (Tenant- und System-DB) anzulegen und nicht nur für den spezifischen Support-Fall. Während der Periode der Inaktivität ist dieser, ähnlich wie der SYSTEM-Benutzer, zu sperren und bei Aktivierung ist ein neues Kennwort bereitzustellen.

Die SAP_INTERNAL_HANA_SUPPORT-Rolle sollte dauerhaft zugewiesen werden. Auf die Wahl des Benutzertypen ist allerdings kein großer Wert zu legen. In einigen Fällen ist es sinnvoll, Zugriff auf das eigene Schema zu haben, z. B. um temporäre Views zwecks Fehleranalyse erstellen zu können.

Man wird allerdings schnell feststellen, dass die Standardrolle nicht immer ausreichend ist. Um einige grundsätzliche Einschränkungen aus dem Weg zu räumen, soll hier eine allgemeine Sammelrolle entwickelt und zugeordnet werden. Der Inhalt der Sammelrolle wäre wie im Folgenden dargestellt.

Lesender Zugriff auf das Repository der Datenbank	.REPO_PACKAGE_ROOT mit REPO.READ EXECUTE auf SYS.REPOSITORY_REST SELECT auf _SYS_REPO Schema
Lesender Zugriff auf XS Admin	Hier kann eine Kopie von den Standardrollen sap.hana.xs.admin.roles::*Viewer genügen

Tabelle 5: Zusatzrollen für SAP Support

Quelle: Eigene Darstellung

Die nächste Stufe im Konzept beinhaltet die applikationsbezogenen „Sonderrechte“, die nur im Bedarfsfall und nur temporär zuzuordnen sind. Diese wären i. d. R. Applikationssupportrollen, welche mit erweiterten Privilegien auf die kundeneigenen Schemas einhergehen.

In dem Anwendungsfall BWonHANA wäre das neben der SAP-HANA-Rolle, die in RS2HANA_VIEW spezifiziert ist, noch zusätzlich eine Rolle mit erweiterten Rechten auf das _SYS_BIC-Schema (siehe SAP-Hinweis 2299622), Leserechten auf einige Tabellen im SAP<*SID*>-Schema sowie u. U. EXECUTE- und DEBUG-Rechten. In diesem Szenario ist darüber hinaus darauf zu achten, dass ein Mapping auf dem SAP-Support-Benutzer in NetWeaver zu gewährleisten ist, der bereits über die nötigen Analyserechte verfügt.

5.3 SAP-Support-Benutzer für XSA

Je nach Art und Komplexität des Support-Falls kann es nötig sein, dem SAP-Support einen User mit weit reichenden Berechtigungen zur Verfügung zu stellen, beispielsweise den XSA_ADMIN.

Für den XSA_ADMIN-User der XSA-Umgebung gelten im Prinzip die gleichen Empfehlungen, wie sie für den SYSTEM-User in HANA gelten. Nach den notwendigen Tätigkeiten in der initialen Einrichtungsphase sollte dieser User gesperrt werden.

> *‚XSA_ADMIN is a first-level administrator user with irrevocable privileges. This user has unlimited access to the Controller and therefore needs to be handled carefully.'*[11]

Der User hat die folgenden XSA-Rollen:

COCKPIT_ADMIN
COCKPIT_CONFIG_TEMPLATE_ADMIN
COCKPIT_RESOURCE_ADMIN
COCKPIT_TROUBLESHOOTING
COCKPIT_USER
COCKPIT_USER_ADMIN
WEBIDE
XS_AUTHORIZATION_ADMIN
XS_CONTROLLER_ADMIN
XS_USER_ADMIN
XS_USER_DISPLAY
XS_USER_PUBLIC

Sinnvoll erscheint es, sowohl einen Support-User als auch einen Administrations-User für den täglichen Betrieb anzulegen, die beide vor allem nicht über XS_CONTROLLER_ADMIN-Rollen verfügen. Auch die drei * ADMIN Role Collections sollten (zumindest im ersten Anlauf) für den Support entbehrlich sein.

6 SAP HANA-Benutzer

6.1 Benutzer SYSTEM

6.1.1 Absicherung des Benutzers SYSTEM

Dem Benutzer SYSTEM sind standardmäßig alle System Privileges zugeordnet. Er verfügt weder über Zugriffsrechte auf die Tabelleninhalte der Tabellen eines SAP-Systems, z. B. SAP ERP oder SAP S/4HANA, noch auf die Schemata von HDI-Containern. Das Kennwort wird während der Installation festgelegt. Er besitzt kein Standardkennwort.

Eine Nutzung im Tagesgeschäft ist nicht erforderlich. Gemäß SAP-Sicherheitsleitfaden sollte der Benutzer nach der Installation und der Einrichtung personifizierter Administrationskonten deaktiviert werden.

[11] https://help.sap.com/viewer/742945a940f240f4a2a0e39f93d3e2d4/2.0.05/en-US/ce30953d48cc4ad1a24d5f9915eedc7f.html?q=xsa_admin.

Mittels des SAP HANA Audit-Logs kann der Benutzer SYSTEM überwacht werden. Hier ist eine spezielle Policy einzurichten, die alle Aktivitäten des Benutzers SYSTEM aufzeichnet. Die Kontrolle dieser Protokolle sollte regelmäßig erfolgen.

Für den Benutzer SYSTEM kann die Sperrung durch Falschanmeldungen deaktiviert werden (Systemparameter indexserver.ini - password policy - password_lock_for_system_user). Hierdurch sind Brute-Force-Attacken auf diesen Benutzer möglich, daher sollte der Parameterwert auf den Standardwert *true* eingestellt bleiben.

6.1.2 Einsatz des SYSTEM User in der Praxis

Bei Miele wird der SYSTEM User möglichst früh nach der initialen Einrichtung eines HANA-Systems gesperrt. Die temporäre Entsperrung kann durch einen User-Admin aus der IT-Security erfolgen oder über einen Notfall-User. Zugriff auf diesen Notfall-User haben die IT-Security und die Datenbankadministratoren.

Benötigt wird der SYSTEM User aktuell nur für ein Update der HANA-Software. Im Umgang mit dem SYSTEM User wird bei Miele nicht zwischen SYSTEMDB und Tenant-DB unterschieden.

Bei der Postbank Systems wird der SYSTEM User ebenfalls gesperrt, sobald ein System in den Betrieb übergeben wird. Die Entsperrung dieses Users ist nur im absoluten Notfall (Ticket, Vier-Augen-Prinzip) bzw. für die genannten Update-Aktivitäten vorgesehen und kann nur vom Firefighter-User-Administrator durchgeführt werden. Entsprechende Aktivitäten werden im Audit-Log mitgeschrieben. Damit die Entsperrung des Nutzers SYSTEM wirklich nur im Extremfall durchgeführt werden muss, wurde aus einer Analyse der Privilegien des SYSTEM User eine Rolle mit sehr weitreichenden Berechtigungen abgeleitet, die dem Firefighter-Administrator zugewiesen ist. Sie enthält alle bekannten Berechtigungen außer den SoD-kritischen Rechten wie etwa USER ADMIN, ROLE ADMIN und Security-Administration.

6.2 SAP-Schema-Owner

Der SAP-Schema-User kann verschiedene Namen haben. Der Default bei Installation mit dem SWPM ist SAPABAP1 bzw. SAPJAVA1. Aber auch SAP<*SID*> ist erlaubt und gängig, allerdings muss man sich vor einer Verwechslung mit dem Betriebssystemuser sap<*sid*> hüten.[12]

6.2.1 Absicherung des SAP-Schema-Owner

Der Schema-Owner existiert in einer HANA-Datenbank, wenn eine ABAP-Applikation (z. B. ERP, S/4HANA) installiert ist. Der Benutzer wird für die Kommunikation mit einem SAP-NetWeaver-System angelegt. Jegliche Kommunikation des SAP-NetWeaver mit der Datenbank erfolgt über diesen Benutzer. Er ist der Besitzer aller Elemente des SAP-

[12] 2535951 – FAQ: SAP HANA Users and Schemas.

Systems und hat somit u. a. Vollzugriff auf alle Tabellen. Die erforderlichen SAP-HANA-Berechtigungen werden ihm automatisch beim Anlegen zugeordnet. Welche Berechtigungen erforderlich sind, listet der SAP-Hinweis 2101316 auf.

Anmeldungen mit diesem Benutzer sind möglich, aber im Tagesgeschäft nicht erforderlich. Dieser Benutzer muss so abgesichert werden, dass Anmeldungen mit ihm möglichst nur nach dem Vier-Augen-Prinzip erfolgen können. Des Weiteren sollten Zugriffe auf die Tabellen seines Schemas protokolliert werden. Hierfür kann eine Auditing-Policy eingerichtet werden. Diese ist folgendermaßen konfiguriert (der Name des SAP-ABAP-Benutzers ist hier SAPP01):

- Audited Actions – DELETE, INSERT, SELECT, UPDATE
- Audited Objects – alle Objekte im Schema SAPP01
- User Excluded from Policy – alle Benutzer außer SAPP01

Diese Policy bewirkt, dass alle Zugriffe per SQL auf die SAP-ABAP-Daten protokolliert werden, außer vom Benutzer SAPP01 selbst. Hier muss evtl. noch ein Backup-Benutzer ergänzt werden.

6.2.2 Zugriff auf SAP-Schema-Owner in der Praxis

Zugriff auf SAP-Schema-Owner haben bei Miele die SAP Basis und die Datenbankadministratoren.

Zugriff auf SAP-Schema-Owner hat bei der Postbank nur die SAP Basis, da hier eine funktionale Trennung zwischen Datenbankadministrationsaufgaben und SAP-Basis-Tätigkeiten vorgesehen ist.

6.3 Restricted User

6.3.1 Einsatz von Restricted Usern

Die Benutzertypen in SAP HANA überschneiden sich mit denen von SAP NetWeaver nur gering. Somit finden wir hier die System-, Service- oder Dialogbenutzertypen nicht, dafür aber die Standard- und die Restricted-Benutzertypen. Der Unterschied zwischen diesen beiden ist zum einen die direkte Zuordnung der PUBLIC-Rolle und zum anderen die CREATE ANY-Berechtigung auf das eigene Datenbankschema. Weil der Restricted User für den Zugriff von Anwendungen auf die Datenbank vorgesehen ist, ist die Anmeldung über die ODBC und JDBC API standardmäßig ausgeschaltet und muss daher explizit erlaubt werden.

Verwendet man den Restricted User nur für Anwendungen, die über http-Aufrufe mit der Datenbank kommunizieren, dann greift man damit zu kurz. Es ist grundsätzlich empfehlenswert, diesen Benutzertyp für alle SAP-HANA-Benutzer zu verwenden. Eine Ausnahme wäre u. a. der Entwicklerzugriff.

Hintergrund des Benutzertyps ist die Anforderung, Entwicklungstätigkeiten außerhalb der Entwicklungsumgebung zu verhindern sowie technischen Benutzern schon von vornherein die Möglichkeit zu nehmen, sich interaktiv über HANA Studio auf die Datenbank anzumelden.

Sollte die Berechtigung notwendig sein, dann kann der Zugriff auf das eigene Schema über den ALTER USER-Befehl zugeordnet werden.

6.3.2 Restricted User in der Praxis

Bei Miele werden aktuell keine Restricted User verwendet. Es ist allerdings auch nur ein HANA-System vorhanden, auf dem User für Anwender abseits der Administratoren eingerichtet sind. Die Anzahl dieser User ist sehr überschaubar.

Beim SAP UCC Magdeburg werden Restricted User für alle technischen administrativen Tätigkeiten wie z. B. Aufräumjobs oder regelmäßige Überprüfungen verwendet, da für diese Nutzer keine Anmeldung erforderlich ist.

7 Technische Benutzergruppen

Benutzergruppen in SAP HANA sind mit dem Release 2.0 SPS02 eingeführt worden. Sie erfüllen den gleichen Zweck wie in SAP NetWeaver, nämlich die Zuständigkeitsverteilung für das Benutzermanagement, und eignen sich nicht für Autorisierungen, Rollenzuweisungen oder die Steuerung des Datenzugriffs. Dies verhält sich anders bei Usern, die über LDAP-Gruppen definiert sind.

7.1 SAP HANA-Benutzergruppen

7.1.1 Funktionsweise

Die Gruppen werden in der Tabelle USERGROUPS gespeichert. Dort lässt sich im Feld IS_USER_ADMIN_ENABLED festlegen, ob weiterhin auch noch die Berechtigung USER ADMIN zur Verwaltung der Benutzer genutzt werden kann. Hiermit kann dann sowohl eine zentrale als auch eine dezentrale Verwaltung von Benutzern eingerichtet werden. Beim Anlegen einer Benutzergruppe wird gesteuert, wie sie berechtigt wird:

Only a group administrator can manage this user group
Nur Benutzer mit dem Object Privilege USERGROUP OPERATOR für diese Gruppe können die Gruppe verwalten.

Both group administrators and user administrators can manage this user group
Zusätzlich zu den Benutzern mit dem Object Privilege USERGROUP OPERATOR können auch Benutzer mit dem System-Privilege USER ADMIN die Gruppe verwalten.

Group creator can manage group
Der Ersteller der Gruppe erhält das Recht zur Verwaltung der Gruppe.

Um Berechtigungen zur Verwaltung einzelner Benutzergruppen zu vergeben, ist die Berechtigung USERGROUP OPERATOR (Privilege) erforderlich. Diese können Sie mit folgendem SQL-Statement zuordnen:

GRANT USERGROUP OPERATOR ON USERGROUP <*Gruppe*> TO <*Benutzer*>

Um beispielsweise dem Benutzer USER1 die Berechtigung zur Verwaltung der Gruppe HANA_ADMIN zu geben, ist folgendes Statement erforderlich:

GRANT USERGROUP OPERATOR ON USERGROUP HANA_ADMIN TO USER1

Damit hat der Benutzer USER1 die Berechtigung, Benutzer in dieser Gruppe anzulegen und zu löschen sowie existierende Benutzer der Gruppe zuzuordnen.

Um die Zuordnung von Benutzern zu Gruppen zu pflegen, verwenden Sie am besten das HANA Cockpit. Dort findet sich das User Group Management im Bereich „Security“ unter der Kachel „User & Role Management“.

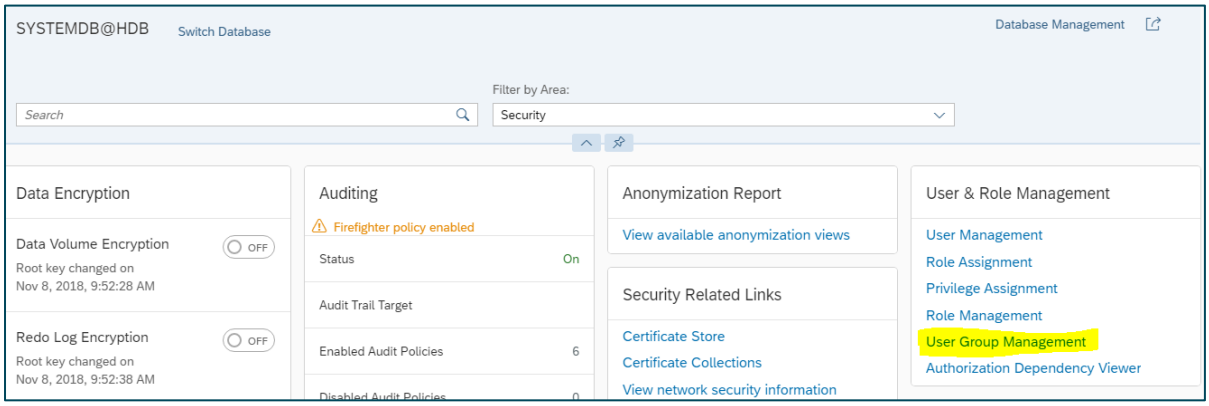


Abbildung 11: Cockpit-Einstieg ins User Group Management

Quelle: Eigene Darstellung

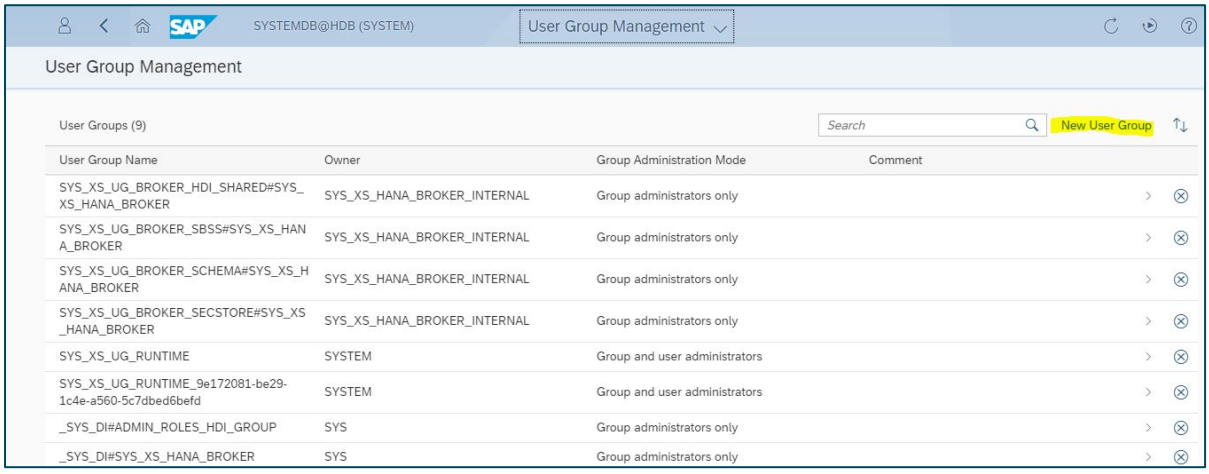


Abbildung 12: Anlage neuer Benutzergruppe

Quelle: Eigene Darstellung

Über die Funktion „New User Group“ kann man eine eigene Gruppe anlegen und zugleich festlegen, welche administrativen Einstellungen für diese Gruppe gewünscht sind.

Beispiel:

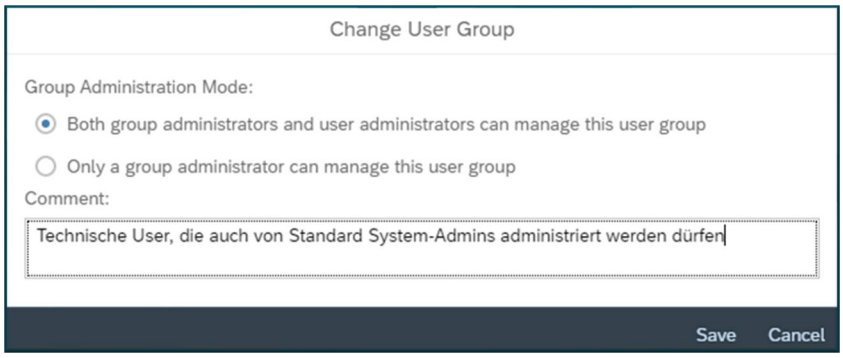


Abbildung 13: Administrationsmodus

Quelle: Eigene Darstellung

Nach Anlegen der User-Gruppe kann das Hinzufügen von Usern sowohl in der Anzeige der Gruppe durchgeführt werden

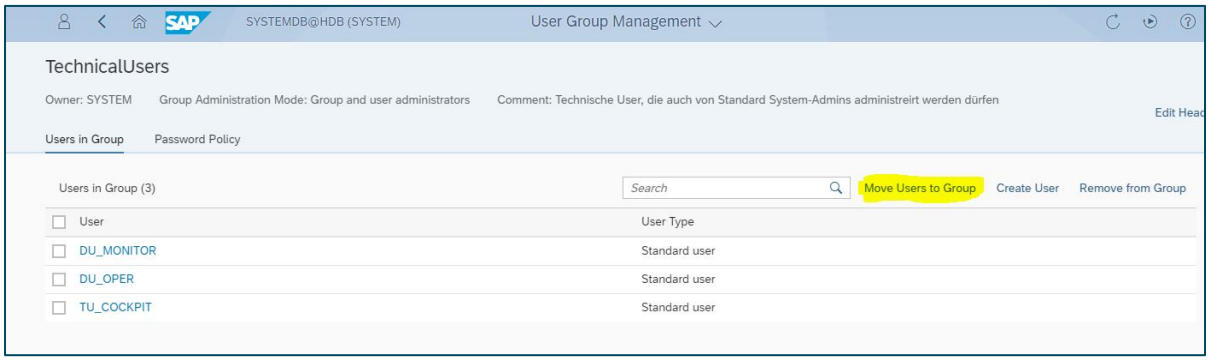


Abbildung 14: Zuordnung über Gruppenadministration

Quelle: Eigene Darstellung

als auch über das User-Management direkt am User-Stammsatz.

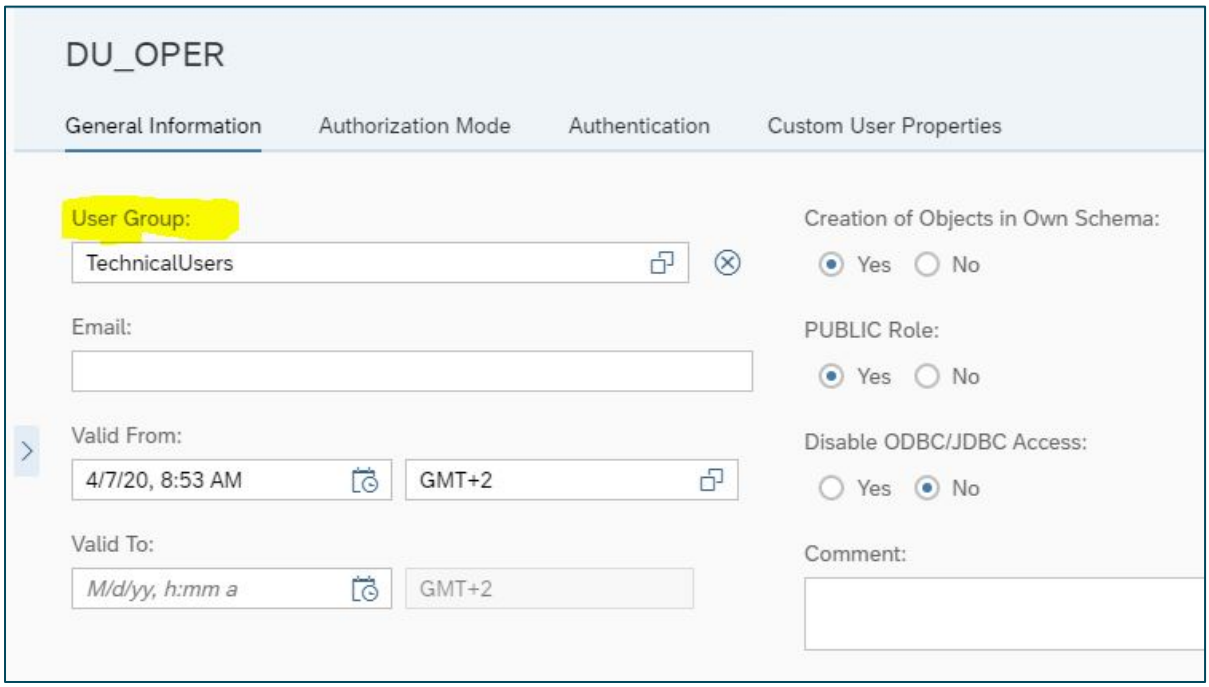


Abbildung 15: Zuordnung über Benutzerstamm

Quelle: Eigene Darstellung

Die Pflege von Benutzergruppen mit SQL ist erforderlich, wenn zur Datenbankadministration das SAP HANA Studio eingesetzt wird. Dieses bietet keine Oberfläche zur Benutzergruppenpflege. Nachfolgend die SQL-Statements zur Pflege von Benutzergruppenzuordnungen:

Anlegen eines Benutzers und Zuordnen zu einer Gruppe:
CREATE USER <*Benutzername*> SET USERGROUP <*Benutzergruppe*>

Benutzer einer anderen Gruppe zuordnen:
ALTER USER <*Benutzername*> SET USERGROUP <*Benutzergruppe*>

Benutzer aus einer Gruppe löschen:
ALTER USER <*Benutzername*> UNSET USERGROUP <*Benutzergruppe*>

7.1.2 Anwendungsgebiete

Ein mögliches Anwendungsgebiet im Hinblick auf die Einhaltung des SoD-Konzepts ist die Umsetzung von getrennten Berechtigungsrollen zur System- und Benutzeradministration, wobei ein Systemadministrator kein USER ADMIN-Privileg besitzt, aber durch Einsatz von Benutzergruppen dennoch zur Sperrung bzw. Entsperrung technischer Benutzer in der Lage ist.

7.2 LDAP-Benutzergruppen

Über eine LDAP-Anbindung kann nicht nur die Authentifizierung der User, sondern auch deren Autorisierung gesteuert werden, denn zwischen Rollen und LDAP-Gruppen

können Zuordnungen erstellt werden. So wird bei erstmaliger Anmeldung mit dem LDAP-Kennwort nicht nur eine Anlage des Users in der HANA-Datenbank ausgelöst, sondern auch automatisch die entsprechende(n) Rolle(n) dem User zugeordnet.

Eine Administration des Users ist dann lokal nicht mehr möglich, er kann lediglich noch gelöscht werden.

Beispiel:

ALTER ROLE DB_SYSTEMDB_ADMIN_C ADD LDAP GROUP 'cn=HANA-Basis,ou=SAP-Hana,ou=APPL,ou=PBGroup,dc=pbcd,dc=bank,dc=de';

Empfehlung: Um hier ein SSO (Single Sign-on) ohne Kennworteingabe zu realisieren, wird für die Anmeldung am Cockpit SAML eingerichtet[13] und der „Absprung“ aus dem Cockpit auf die Zieldatenbank wird mit einem JWT-Ticket realisiert.

Beispiel:

Anmeldung am Cockpit über SAML (keine Eingabe von Username/Password).

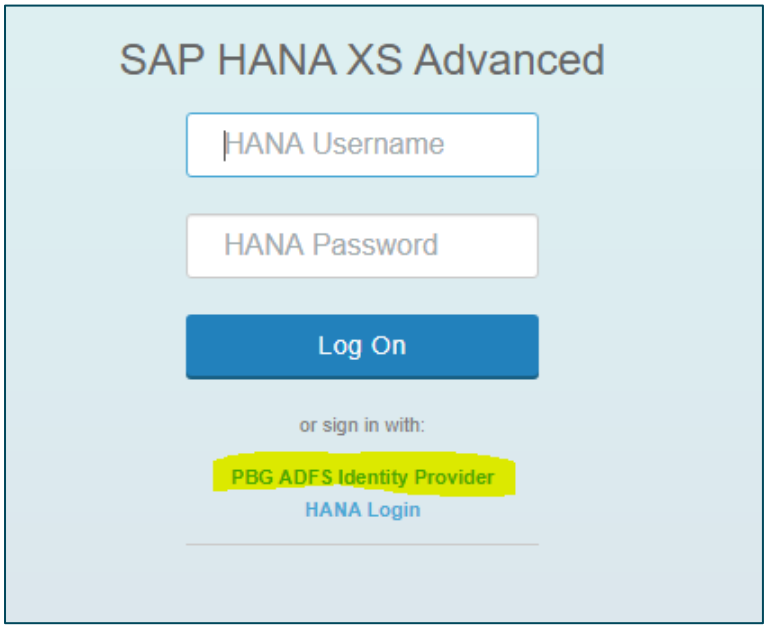


Abbildung 16: Cockpit Anmeldemaske mit SAML

Quelle: Eigene Darstellung

[13] https://launchpad.support.sap.com/#/notes/2770777.

Im Resource Directory kann als Credentials „SSO Enabled“ ausgewählt werden. (Auch hier erneut keine Eingabe von Username/Password).

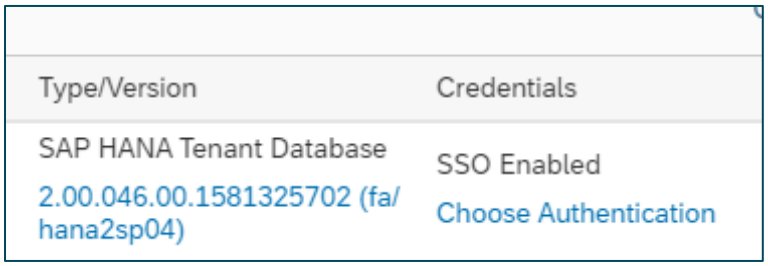


Abbildung 17: SSO Credentials im Cockpit

Quelle: Eigene Darstellung

Voraussetzung ist, neben der Einrichtung des IDP für die JWT-Tickets (das ist hier das Cockpit selbst), die Definition dieser Authentifizierung am Benutzerstamm.

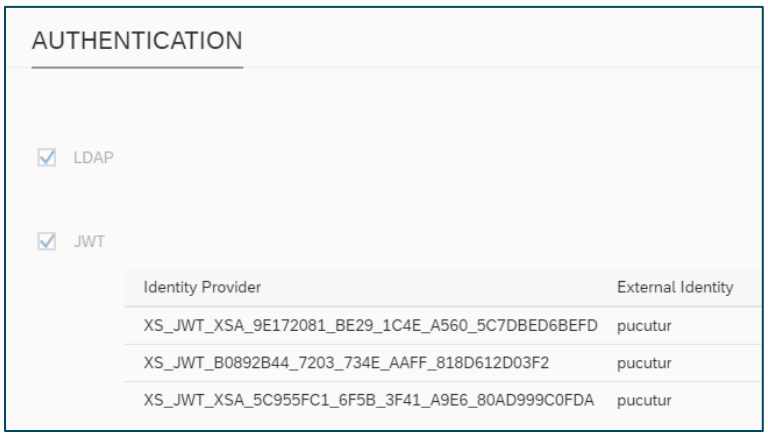


Abbildung 18: Authentifizierungsmethoden

Quelle: Eigene Darstellung

8 Analysemöglichkeiten in SAP HANA

8.1 Rollen und Berechtigungen

8.1.1 Auswertungen mit SAP HANA-Views

SAP HANA beinhaltet verschiedene Standard-Views, mit denen Benutzer, Rollen und Berechtigungen analysiert werden können. Mit den nachfolgenden Views werden effektive Berechtigungen (= unabhängig von der Art der Zuordnung) ausgewertet.

- EFFECTIVE_APPLICATION_PRIVILEGES
  Wertet die einem Benutzer effektiv zugeordneten Application Privileges aus. Beim Aufruf muss ein Benutzername in der WHERE-Klausel angegeben werden.
- EFFECTIVE_MASK_EXPRESSIONS

Wertet aus, wie Benutzer auf maskierte Daten zugreifen dürfen. Hiermit kann u. a. das Privilege UNMASKED (unmaskierte Anzeige von Daten) ausgewertet werden.

- EFFECTIVE_PRIVILEGE_GRANTEES
  Wertet aus, welchen Benutzern und Rollen eine bestimmte Berechtigung zugeordnet ist. Unter anderem kann analysiert werden, welchen Benutzern und Rollen bestimmte System-Privileges zugeordnet sind.
- EFFECTIVE_PRIVILEGES
  Wertet aus, welche Berechtigungen einem Benutzer effektiv zugeordnet sind. Es werden auch die Privileges aufgelistet, die durch Rollen zugeordnet sind. Beim Aufruf der View muss ein Benutzername in der WHERE-Klausel angeben werden.
- EFFECTIVE_ROLE_GRANTEES
  Wertet aus, ob eine Rolle einem Benutzer oder einer anderen Rolle effektiv zugeordnet ist. Als Selektion ist der Rollenname anzugeben.
- EFFECTIVE_ROLES
  Wertet aus, welche Rollen einem Benutzer effektiv zugeordnet sind (also auch durch andere Rollen). Beim Aufruf muss ein Benutzername in der WHERE-Klausel angeben werden.
- EFFECTIVE_STRUCTURED_PRIVILEGES
  Wertet die einem Benutzer effektiv zugeordneten Analytic Privileges aus. Beim Aufruf muss ein Benutzername in der WHERE-Klausel angeben werden.

In der *SAP HANA SQL and System Views Reference* ist der Aufbau der Views beschrieben:

https://help.sap.com/viewer/4fe29514fd584807ac9f2a04f6754767/2.0.04/en-US

In der Praxis erstellen sich viele Unternehmen eigene Infosysteme, indem sie mithilfe der Views einzelne Berechtigungsabfragen definieren und diese dann jeweils abspeichern. So können immer wiederkehrende Fragestellungen mit wenig Aufwand beantwortet werden. Die einzelnen Abfragen werden häufig auch zu Skripten zusammengestellt, sodass verschiedene Berechtigungsanalysen mittels eines einzigen Skripts durchgeführt werden können.

8.1.2 Auswertungen mit der SQL-Statement-Library

SAP liefert vordefinierte Skripte für verschiedene Analysen aus. Diese sind als Anhang zum SAP-Hinweis 1969700 erhältlich. Im SAP HANA-Database-Explorer sind sie in der Statement-Library integriert. Neben den *Mini Checks* (vordefinierte Security-Checks zum Leitfaden *SAP HANA Security Checklists and Recommendations)* können mit dem Skript *HANA_Security_GrantedRolesAndPrivileges* – verfügbar für verschiedene HANA-Release-Stände – Berechtigungen ausgewertet werden. Das Skript enthält einen Bereich für Selektionen (*/* Modification section */*), wodurch

Auswertungen zu allen Fragestellungen zu Berechtigungen möglich sind. In der Praxis werden mit diesem Skript häufig komplexe Fragestellungen abgebildet, welche dann jeweils als Vorlage abgespeichert werden. Dies erleichtert regelmäßige Analysen vergebener Berechtigungen.

8.1.3 Auswertungen mit PUBLIC SYNONYMS

Neben den Views können auch tabellarische Sichten für Analysen genutzt werden. Diese werden mit der Rolle PUBLIC berechtigt.

- GRANTED_ROLES
  Listet auf, welche Rollen anderen Rollen und Benutzern zugeordnet sind
- ROLES
  Übersicht über alle im System vorhandenen Rollen
- GRANTED_PRIVILEGES
  Listet auf, welche Privilegien Rollen und Benutzern zugeordnet sind
- OBJECT_PRIVILEGES
  Übersicht über alle im System vorhandenen Privilegien nach Objekttyp
- PRIVILEGES
  Übersicht über alle im System vorhandenen Privilegien nach Privilegientyp
- STRUCTURED_PRIVILEGES
  Übersicht über alle im System vorhandenen analytischen Privilegien

8.1.4 Auswertung inaktiver Repository-Rollen

Repository-Rollen müssen aktiviert werden, bevor Änderungen wirksam werden. Zur Kontrolle, ob alle Rollen korrekt aktiviert wurden, kann die Tabelle _SYS_REPO.INACTIVE_OBJECT genutzt werden. Dort werden alle nicht aktivierten Repository-Objekte gespeichert. Mit folgendem SQL-Statement listen Sie alle inaktiven Rollen auf:

```
select * from _SYS_REPO.INACTIVE_OBJECT where OBJECT_SUFFIX = 'hdbrole'
```

Eine Auflistung aller aktiven Objekte erhalten Sie über die Tabelle _SYS_REPO.ACTIVE_OBJECT.

8.2 Sicherheitsrelevante Alerts

Der Statistics-Service in SAP HANA sammelt kontinuierlich Daten des Systems und wertet sie nach vordefinierten Kriterien und Zeiträumen aus. Werden hierbei Fehler festgestellt, so wird eine Alarmmeldung erzeugt. Neben den Auswertungen zur Überwachung der Performance und des Ressourcenverbrauchs werden auch sicherheitsrelevante Alarmmeldungen erzeugt.

Es kann z. B. der SAP Solution Manager eingesetzt werden, um die Early-Watch-Alerts der HANA-Datenbanken auszuwerten und entsprechende Incident-Tickets zu generieren.

Die nachfolgende Tabelle listet wesentliche sicherheitsrelevante Alerts auf. Weitere Informationen (u. a. zur Auswertung der Alerts und zur Definition von Schwellenwerten zur Alert-Generierung) finden Sie im SAP HANA Administration Guide im Kapitel *System Administration/Monitoring the SAP HANA Database/Monitoring in SAP HANA Cockpit/ Alerts and Diagnostics*:

IDD	Name	Beschreibung	Kategorie
31	License expiry	Abgelaufene Lizenzen; Details im View M_LICENCE	1 Diagnosis Files
34	Unavailable volumes	Datenträger ist nicht verfügbar.	5 Configuration
35	Existence of data backup	Es existiert kein Backup, somit kein Recovery möglich.	7 Backup
39	Long-running statements	Lange Laufzeit eines SQL-Statements. Detaillierte Informationen dazu im View _SYS_STATISTICS.HOST_LONG_RUNNING_STATEMENTS	6 Sessions/ Transactions
49	Long-running blocking situations	Lange andauernde Sperren an. Evtl. müssen Transaktionen abgebrochen werden.	6 Sessions/ Transactions
57	Instance secure store file system (SSFS) inaccessible	Verfügbarkeit des SSFS (Secure Store in the File System)	9 Security
62	Expiration of database user passwords	Zeigt Benutzer mit abgelaufenem Kennwort an.	9 Security
63	Granting of SAP_INTERNAL_ HANA_SUPPORT role	Zuordnung der Rolle SAP_INTERNAL_HANA_SUPPORT	9 Security
64	Total memory usage of table-based audit log	Hauptspeicherverbrauch der Tabellen mit Audit-Log-Einträgen.	2 Memory

IDD	Name	Beschreibung	Kategorie
84	Insecure instance SSFS encryption configuration	Änderungen des Master-Key des SSFS	9 Security
85	Insecure systemPKI SSFS encryption configuration	Änderungen des Master-Key der PKI SSFS	9 Security
86	Internal communication is configured too openly	Sichere Konfiguration der Ports für die interne Kommunikation (Hinweis 2183363)	9 Security
87	Granting of SAP HANA DI support privileges	Vergabe von Support-Privileges für die HDI (HANA Deployment Infrastructure)	9 Security
97	Granting of SAP HANA DI container import privileges	Zuordnung von Berechtigungen zum Import von HDI-Container	9 Security
102	Existence of system database backup	Fehlendes Backup der Systemdatenbank, somit ist kein Recovery möglich	7 Backup
101	SQL access for SAP HANA DI technical user	Berechtigungen für Zugriff per SQL für technische HDI-Benutzer	9 Security
103	Usage of deprecated features	Nutzung veralteter Funktionen (SAP-Hinweis 2425002)	0 Other
128	LDAP Enabled Users without SSL	Zeigt an, ob ein Benutzer für die LDAP-Authentifizierung aktiviert ist und SSL ausgeschaltet ist (Risiko von Man-in-the-Middle-Angriffen)	2 Security

Tabelle 6: Sicherheitsrelevante Alerts

Quelle: SAP HANA Troubleshooting and Performance Analysis Guide, SAP HANA Platform 2.0 SPS04

8.3 Sicherheitsrelevantes Tracing

8.3.1 Berechtigungstraces

Der **Authorization Dependency Viewer** für Berechtigungen im HANA Cockpit ist ein mächtiges Tool zur Analyse fehlender Berechtigungen durch Darstellung der Abhängigkeiten.

Beispiel:

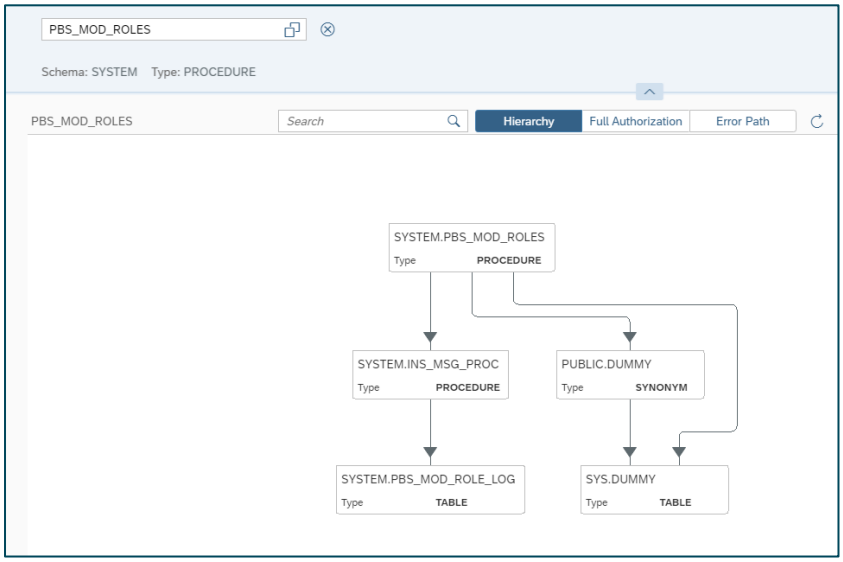


Abbildung 19: Authorization Dependency Viewer

Quelle: Eigene Darstellung

- Authorization Error Collection: Prozedur für GUID, um festzustellen, welches Statement den Fehler erzeugt
- Seit SAP HANA 2.0 SPS4 wird bei fehlenden Berechtigungen eine GUID ausgegeben
  - SYS.GET_INSSUFICIENT_PRIVILEGE_ERROR_DETAILS(<GUID>,?);
  - Um die Prozedur ausführen zu können, muss die EXECUTE-Berechtigung vom SYSTEM-Benutzer vergeben werden
- Trace (User-spezifisch)
  Wird beispielsweise im Database-Explorer eingeschaltet

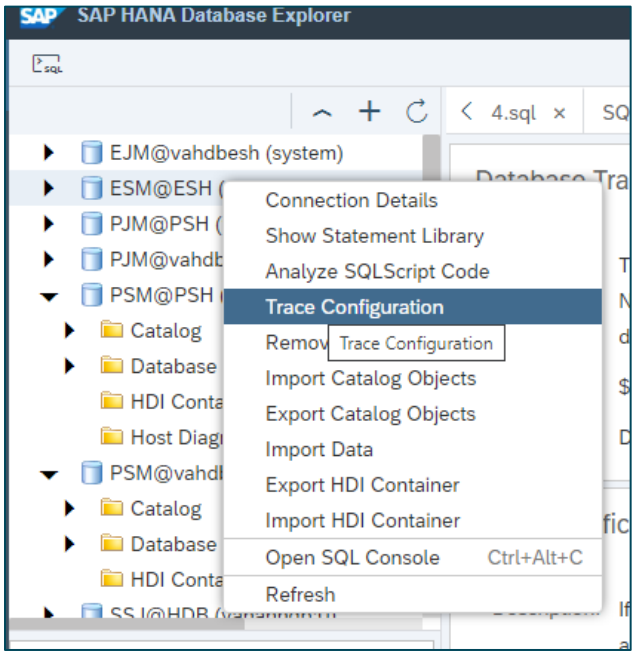


Abbildung 20: Trace Konfiguration im Database Explorer

Quelle: Eigene Darstellung

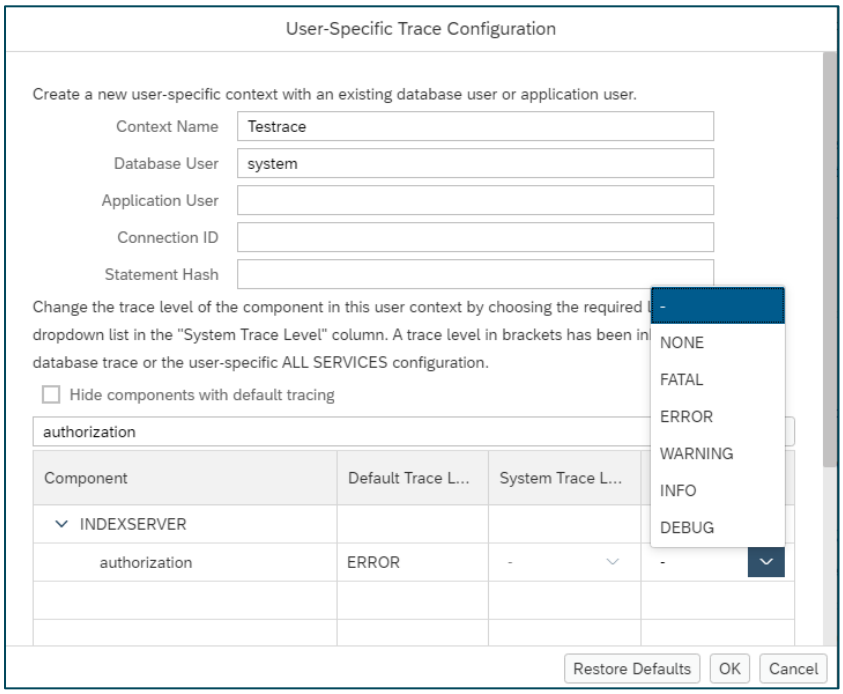


Abbildung 21: Benutzerspezifische Tracekonfiguration

Quelle: Eigene Darstellung

- SYS-View: Ownership eines DB-Objekts nachsehen
  - Für Schema: PUBLIC.SCHEMAS
  - Für alle anderen Objekte: PUBLIC.OWNERSHIP

8.3.2 Analysemöglichkeiten von HTTP basierten Fehlern

In SAP HANA stehen unter anderem folgende sicherheitsrelevante Trace-Optionen zur Verfügung:[14]

Developer Trace
Trace-File webdispatcher_<*host*>.<*port*>_dev_webdisp:

- DB Trace level dev_webdisp-Komponenten des Webdispatcher-Service ändern

```
level: FATAL, ERROR, WARNING, INFO, DEBUG
alter system alter configuration
('webdispatcher.ini','SYSTEM')SET
('trace','dev_webdisp')='<level>' with reconfigure;
```

- Ändern der Sektion rdisp/trace in der webdispatcher.ini auf die level-Werte

```
0/1/2/3 alter system alter configuration
('webdispatcher.ini','SYSTEM') set
('profile','rdisp/TRACE')='<level>' with reconfigure;
```

DB-Trace
Trace-Files:

- webdispatcher_<*host*>.<*port*>.<*3_digit_file_counter*>.trc
- webdispatcher_alert.<*host*>.trc

Trace-Aktivierung durch Anpassung des Trace-Levels der Web Dispatcher-Komponente des Web Dispatcher-Service

Header-Trace

Hinzufügen des Wertes icm/http/trace_info in der [profile]-Sektion der webdispatcher.ini auf true

```
alter system alter configuration
('webdispatcher.ini','SYSTEM') set
('profile','icm/HTTP/trace_info')='TRUE' with reconfigure;
```

- Header-Trace-Informationen werden im dev_webdisp Tracefile niedergeschrieben

HTTP-Access-Log

Für das Loggen aller HTTP(S)-Zugriffe muss folgender Wert in der webdispatcher.ini hinzugefügt werden:

[14] https://launchpad.support.sap.com/#/notes/2697007.
Für XSA-Applikationen: https://launchpad.support.sap.com/#/notes/2201212.
Hinweis “2119087 - How-To: Configuring SAP HANA Traces” beinhaltet eine umfassende Zusammenfassung aller Trace-Möglichkeiten.

- =day, LOGFORMAT=SAP
- Das Logfile ist unter access_log-<*Zeitstempel*> zu finden

9 Massenoperationen

9.1 Kopieren von Benutzern und Rollen

Benutzer können nicht, wie in ABAP, mit all ihren Berechtigungen kopiert werden. Zum Beispiel können Berechtigungen auf Katalogobjekte nur weitergegeben werden, wenn der kopierende Benutzer selbst über diese Rechte verfügt. Das SAP HANA Cockpit bietet keine Standardfunktion zum Kopieren von Benutzern. In SAP HANA Studio besteht die Möglichkeit, Benutzer mit ihren Repository-Rollen zu kopieren, siehe SAP-Hinweis 2621987 (Copy user with system privileges and objects privileges). Katalogrollen und zugeordnete Privileges werden nicht kopiert.

Um das Kopieren von Privileges zu ermöglichen, kann das Skript **HANA_Security_CopyPrivilegesAndRoles_CommandGenerator_2.00.000+** genutzt werden. Dies ist in der Anlage zum SAP-Hinweis 1969700 enthalten. Im SAP HANA-Database-Explorer kann das Skript über die **Statement Library** aufgerufen werden. Dieses Skript generiert SQL-Statements, mit denen die kopierbaren Elemente (Katalogrollen, Object Privileges und Package-Privileges) einem anderen Benutzer zugeordnet werden können. Privileges, Analytic Privileges und Application Privileges können nicht kopiert werden. Zum Kopieren von Rollen kann das Skript ebenfalls genutzt werden.

Im Block /* Modification section */ des Skripts können folgende Selektionen angegeben werden:

- SOURCE_GRANTEE
  Benutzer oder Rolle, deren Rollen und Berechtigungen kopiert werden sollen
- TARGET_GRANTEE
  Benutzer oder Rolle, dem die Rollen und Berechtigungen zugeordnet werden sollen
- GRANT_ROLES
  X = Rollen, die kopiert werden sollen
  ' ' = Rollen, die nicht kopiert werden sollen
- GRANT_PRIVILEGES
  X = Privilegien, die kopiert werden sollen
  ' ' = Privilegien, die nicht kopiert werden sollen

Nachfolgendes Listing zeigt beispielhaft, dass die Rollen und Berechtigungen des Benutzers USER1 zum Benutzer USER2 kopiert werden sollen.

- (SELECT /* Modification section */
- 'USER1' SOURCE_GRANTEE,
- 'USER2' TARGET_GRANTEE,
- 'X' GRANT_ROLES,
- 'X' GRANT_PRIVILEGES

Das Skript erzeugt nun einzelne SQL-Statements. Mit diesen können die Privileges und Rollen kopiert werden. Es werden nur Statements für die Privileges und Rollen erzeugt, für die der zu kopierende Benutzer das Recht *Grantable to others* besitzt. Es können nur die Statements ausgeführt werden, für die der ausführende Benutzer selbst auch die Berechtigungen besitzt. Andernfalls wird die Fehlermeldung *insufficient privilege: Not authorized* ausgegeben.

9.2 Temporäres Sperren von Benutzern

Ist es erforderlich, dass alle Nichtadministrationsbenutzer gesperrt werden (z. B. zu Wartungszwecken), bietet der SAP-Hinweis 1986645 („Nur Administrationsbenutzer sollen in HANA-Datenbank arbeiten dürfen“) hierfür Unterstützung. Er stellt Prozeduren zur Verfügung, mit denen Massensperrungen und -entsperrungen von Benutzern möglich sind. Diese befinden sich im Anhang in der Datei SESSION_ADMIN_ONLY.sql.

Mit den Prozeduren können offene Sitzungen von Benutzern geschlossen werden. Danach können die Benutzer gesperrt werden. Benutzer werden nicht gesperrt, wenn sie:

- das Systemprivileg SESSION ADMIN besitzen,
- in einer Ausnahmetabelle hinterlegt wurden,
- bereits gesperrt sind.

Die gesperrten Benutzer werden dann in eine Tabelle geschrieben. Nur die Benutzer in dieser Tabelle werden dann auch wieder entsperrt. Dadurch wird gesichert, dass Benutzer, die vorher gesperrt waren, auch gesperrt bleiben.

9.3 Post-Copy Automation (PCA) for SAP HANA

Eine Systemkopie kann zu unterschiedlichen Verwendungszwecken erstellt werden. Ein Beispiel ist, die Kopie eines Produktivsystems als zukünftiges System zur Qualitätssicherung einzusetzen, da wir durch die Kopie im Hinblick auf die Datengrundlage ein identisches System zum Testen unserer Entwicklungen bekommen. Bei einer Systemkopie sind je nach Szenario unterschiedliche Systeme involviert. Da sich Einstellungen, Benutzer/Berechtigungen und Systemverbindungen zwischen den Systemen mit hoher Wahrscheinlichkeit unterscheiden werden, sind im Nachgang oft weitere Schritte notwendig, um den „alten Zustand“ der zuvor genannten Punkte wiederherzustellen.

Werden bei der Systemkopie eines Applikationsservers schon etliche Tools zur Automatisierung manueller Nacharbeiten angeboten, wie z. B. die von SAP angebotene SAP Landscape Management Software (kurz LaMa), wird für eine SAP HANA-Datenbank auch auf SAP-Seite aktuell keine Software zur Post-Copy Automation angeboten.

Zu dem Thema gibt es auch bereits zwei bekannte „Feature Requests“, die an SAP gestellt worden sind:

- https://influence.sap.com/sap/ino/#/idea/214930
- https://influence.sap.com/sap/ino/#/idea/242029

Die Diskussion zum Thema kann aktuell im DSAGNet eingesehen werden:

Zum Beitrag: HANA-Benutzer vor Systemkopie „retten“

Eine mögliche Lösung in Form einer Eigenentwicklung, die bereits bei den Stadtwerken München produktiv im Einsatz ist, wird in den folgenden Abschnitten konzeptionell vorgestellt:

Es handelt sich bei der Lösung um eine Reihe manueller sowie teilautomatisierter Schritte, die durch Unterstützung diverser Datenbankprozeduren abgearbeitet werden müssen.

Das Gesamtkonzept sieht demnach wie folgt aus:
(Voraussetzung: gleicher Entwicklungsstand)

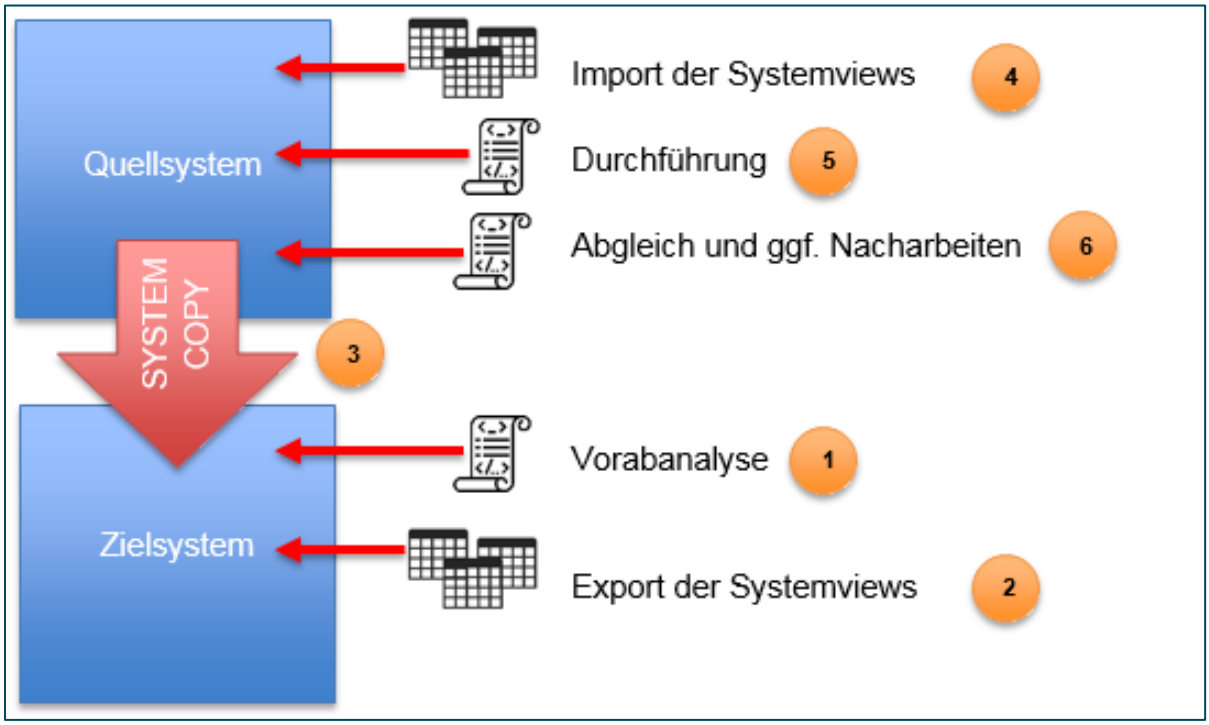


Abbildung 22: Gesamtkonzept Post-Copy Automation

Quelle: Eigene Darstellung

Es werden die folgenden Systemviews exportiert:

- "SYS"."USERS"
- "SYS"."REMOTE_USERS"
- "SYS"."GRANTED_ROLES"
- "SYS"."GRANTED_PRIVILEGES"
- "SYS"."REMOTE_SOURCES"
- "SYS"."CREDENTIALS"

Die dort enthaltenen Informationen reichen für eine vollständige Wiederherstellung der Benutzer, deren Rollen und Berechtigungen sowie der aktuell angelegten Systemverbindungen aus.

Einzige Einschränkung: Die Übernahme des Passworts aus dem Zielsystem ist aktuell aus Sicherheitsgründen architekturbedingt nicht möglich. Es muss daher neu gesetzt werden!

Über eine Customizing-Tabelle lassen sich technische Benutzer definieren, die in der aktuellen Lösung nicht automatisiert verändert werden.

Personalisierte Benutzer werden vorab alle gelöscht und danach entsprechend neu angelegt sowie mit den vorher zugewiesenen Berechtigungsrollen ausgestattet.

Aktuelle Nacharbeiten:

- erneute Vergabe von zuvor zugewiesenen Einzelprivilegien (teilautomatisiert mit Prozedur)
- ggf. manuelles Anlegen / Neuanlegen vorhandener SDA-Verbindungen
- ggf. manuelles Anlegen technischer Benutzer, falls diese auf dem Quellsystem nicht existiert haben

Idee für Weiterentwicklung:

- weitere Automatisierung mithilfe von hdbsql auf Betriebssystemebene
- automatisiertes Anlegen der SDA-Verbindungen

9.4 Anlegen von Benutzern und Rollen mithilfe von Python

Für den Prozess des initialen Anlegens von Benutzern und Rollen kann es sinnvoll sein, diese Schritte zu automatisieren. Wir haben dies mithilfe eines Python-Skripts umgesetzt. Die Verbindung zur Datenbank wird mittels der SAP-eigenen Library hdbcli aufgebaut. Diese Library kann auch für das Absetzen anderer SQL-Befehle zur Datenbank genutzt werden. Das Skript haben wir aufgrund der Länge an dieses Dokument angefügt und nicht in das Dokument integriert.

Das Skript kann ohne Parameter gestartet werden oder mit der Übergabe von optionalen Parametern. Durch Übergabe der Parameter kann das Skript auch automatisch laufen oder zu eingeplanten Zeiten. Eine Übersicht über alle Parameter wird angezeigt mittels: ./HPS.py -h.

Bei jeder Ausführung des Skripts wird eine Log-Datei geschrieben. Diese wird in den /tmp-Ordner geschrieben, Name und Speicherort können angepasst werden unter dem Kommentar ***„# configure log file“.***

Standardmäßig erfolgen alle Operationen auf der SYSTEMDB, möchte man eine Tenant-Datenbank bearbeiten, muss man den optionalen Parameter -t mit übergeben.

Falls ein Nutzer bereits existiert, wird dieser entsperrt und wieder aktiviert und es werden ggf. fehlende Rollen zugewiesen.

Roles.json

Die Informationen für die anzulegenden Nutzer und Rollen werden aus einer zugehörigen Konfigurationsdatei Roles.json eingelesen, sodass diese möglichst einfach konfigurierbar sind.

Die anzulegenden Nutzer werden im Bereich „users“ festgelegt. Ein Nutzer besteht aus einem Nutzernamen, Rollen, die zugewiesen werden sollen, und einem Passwort.

Die Rollen sind unter dem Abschnitt „roles“ der Nutzer aufgeführt. Diese können bei Bedarf als Grantable vergeben werden. Dies wird gekennzeichnet durch den Parameter false hinter dem Rollennamen. Rollen bestehen aus einem Rollennamen und den verschiedenen Privilegien. Momentan unterstützt sind folgende Privilegien:

- system privileges
- static roles
- dynamic roles
- object privileges (table, schema)

Die einzelnen Privilegien können auch wieder als Grantable vergeben werden, angezeigt durch den Parameter false hinter dem jeweiligen Privileg.

Standardmäßig wird das Passwort der Nutzer auf das gleiche Passwort des verwendeten Administrationsnutzers gesetzt. Angezeigt wird dies durch den Parameter DEFAULT, der administrative Nutzer ist im Standard auf SYSTEM gesetzt, da wir davon ausgehen, dass das Skript hauptsächlich bei leeren Systemen genutzt wird, die gerade erst eingerichtet werden. Dieser Parameter kann optional mitgegeben werden, um einen eigenen Nutzer zu verwenden.

Im Folgenden wird beispielhaft der Aufbau einer Roles.json -Datei gezeigt:

```
{
      "users": {
            "BACKUP": {
                  "roles": {
                        "BACKUP_ROLE": false
                  },
                  "password":"DEFAULT"
         },
            "HANACLEANER":{
                  "roles":{
                        "HANACLEANER_ROLE": false
                  },
                  "password":"DEFAULT"
         }
      },
      "roles": {
            "HANACLEANER_ROLE": {
                  "SYSTEM_PRIVILEGES": {
                        "BACKUP ADMIN": false,
                        "AUDIT ADMIN": false,
                        "AUDIT OPERATOR": false,
                        "CATALOG READ": false,
                        "LOG ADMIN": false,
                        "MONITOR ADMIN": false,
                        "RESOURCE ADMIN": false,
                        "TRACE ADMIN": false
                  },
                  "OBJECT_PRIVILEGES": {
                        "TABLE": {

      "_SYS_STATISTICS.HOST_OBJECT_LOCK_STATISTICS_BASE": {
                                    "SELECT": false,
                                    "DELETE": false
                              },

      "_SYS_STATISTICS.STATISTICS_ALERTS_BASE": {
                                    "SELECT": false,
                                    "DELETE": false
                              }
                        }
                  }
         },
            "BACKUP_ROLE": {
                  "SYSTEM_PRIVILEGES": {
                        "BACKUP ADMIN": false
                  }
                        }
      }
}
```

Impressum

Wir weisen ausdrücklich darauf hin, dass das vorliegende Dokument nicht jeglichen Regelungsbedarf sämtlicher DSAG-Mitglieder in allen Geschäftsszenarien antizipieren und abdecken kann. Insofern müssen die angesprochenen Themen und Anregungen naturgemäß unvollständig bleiben. Die DSAG und die beteiligten Autoren können bezüglich der Vollständigkeit und Erfolgsgeeignetheit der Anregungen keine Verantwortung übernehmen.

Deutschsprachige SAP® Anwendergruppe e. V.
Altrottstraße 34 a
69190 Walldorf | Deutschland
Telefon +49 6227 35809-58
Telefax +49 6227 35809-59
E-Mail info@dsag.de
dsag.de