Revision

Vortrag im AK IV-Rev

S/4 HANA – Grundsätzliche Bedingungen zur Berechtigungssteuerung

enercity Konzernrevision (KR)

2023

enercity
positive energie

Einleitung

- S/4 HANA ist in aller Munde. Wer seine Prozesse in die Zukunft führen möchte und auch datenintegrativ voranschreiten mag, kommt an S/4 HANA nicht vorbei.
- Dabei muss festgestellt werden, dass die In-Memory-Fokussierung der große Wurf ist, wenn auch SAP nicht der Erste ist, der sich mit diesem Konzept in neue Höhen schwingt.
- Der nachfolgende Vortrag im Arbeitskreis IV-Revision der Energieversorger soll die grundsätzlichen Aspekte der Berechtigungssteuerung bei einem Umsetzungsprojekt kurz erörtern und nicht in Vollständigkeit die Steuerung der Berechtigungen darstellen.
- Allerdings wird sehr leicht ersichtlich, dass weder ein Umstieg schnell von der Hand geht noch die Kontinuität des sicheren bzw. Compliance-konformen Einsatzes einfach sein wird. Die Ebenen zum klassischen ABAP-Stack-SAP haben sich verändert, sind eher gewachsen und diffizil für die Administration und das Prüfwesen.

SAP Fiori

- S/4 HANA // HANA-DB mit In-Memory-Technologie, Daten gehalten im Arbeitsspeicher, schneller Zugriff auf große Datenmengen
- bei „Gemischtbetrieb“ auch geteilte Berechtigungen – klassisch über Transaktionen **und** Fiori
- Größte Herausforderung: **SAP Fiori Apps**! Viele Transaktionen werden weiterhin genutzt, neue Funktionen von SAP werden aber nicht mehr transaktional bereitgestellt, sondern nur noch als SAP Fiori Apps.
- Notwendig: App-Installation und Frontend- und Backend-Berechtigungen müssen ausgestaltet werden. App-Berechtigungen sind also nicht mehr transaktional, vielmehr Serviceberechtigungen, sodass sie nicht mehr per GUI-Oberfläche aufgerufen werden können.
- Daher Kachelkataloge, die individuell angepasst werden müssen => hoher Aufwand
- Standard-Kachel-Kataloge stehen funktional zur Verfügung. Moderne Sicht auf die Funktionen, aber hoher Anpassungsbedarf.

Technik

- Kein unmittelbarer Zugriff aus dem Browser heraus auf die S/4 HANA Ebene, sondern auf den Frontend-Server der S/4 HANA Bereitstellung.
- Frontend-Server mit Verbindung zum Fiori Launchpad, nimmt Anforderungen der User entgegen und bereitet die Verbindung zum Backend, Backend = S/4 HANA, Anwender melden sich nicht direkt ins Backend, sondern am Frontend-Server an, gesicherte RFC-Verbindung, so Absicherung über Gateway
- Auf dem Frontend werden die Kachel-Apps als Frontend-Versionen berechtigt, darüber ist die jeweilige App enabled oder disabled. Wird Zugriff gewährt, wird die zugehörige Backend-App durch die Frontend-App aufgerufen.
- Erst jetzt erfolgen die Berechtigungsprüfungen. Bekannte, ehemalige Transaktionscodes (aus der Steuerung über Berechtigungsobjekt S_TCODE) existieren bei Fiori Apps nicht. Es gibt aber nicht nur ausschließlich Fiori Apps, sondern auch umgesetzte **Legacy Apps**, also prozessual identische Transaktionen mit sämtlichen Steuerungen ehemaliger Anforderungen.

PFCG

- PFCG existiert noch. In der PFCG geht es um Frontend- und Backend-Berechtigungen. Man hat also eine PFCG und somit ein Menü, jedoch lädt man sich nun keine Transaktionen mehr, sondern Apps herunter. Aber es gibt eben die Möglichkeit, einen Mischbetrieb zu fahren, in dem die Legacy Apps weiter als Transaktionen genutzt werden.
- Dies entspricht einer nicht unerheblichen Aufwandsreduzierung. Vorsichtig muss man damit aber trotzdem sein. Dies bedeutet, dass zwar die PFCG für die Fiori-Apps (> 2.000 Apps) benötigt wird, aber für die meisten Prozessaufrufe (>10.000 Legacy Apps) in der S/4-Umgebung können auch weiterhin analoge Transaktionen genutzt werden.

Zugriffsmodell der Kacheln

- Der Zugriff auf die Kacheln als Zugangskriterium muss für die User (rollen) definiert werden. Entsprechend werden Gruppen mit den aufgabenbezogen-notwendigen Kacheln (Kachelgruppen) definiert.
- SAP bietet aufgabenbezogene Standardkachelgruppen an, diese müssen allerdings nahezu immer angepasst werden. Zusätzliche Gruppen bleiben unausweichlich.
- In die Aufgabenrolle werden folgend keine Apps, sondern Kachelgruppen hineingezogen. Zusätzlich dazu gibt es die Kachelkataloge, in denen die Technikzugänge stehen, also was für ein Service darunter liegt. Später liegen dort auch die Berechtigungsobjekte. Folglich werden zwei differente Elemente zur Steuerung des Zugriffs benötigt, bis klar ist, welche Rechte jemand aus seiner Aufgabenrolle heraus tatsächlich erhält.
- Ist aber die Zuweisung zu einer Aufgabenrolle, die Kachelgruppen und Kachelkataloge beinhaltet, bei einem User gegeben, sieht dieser in seinem Frontend alle darin enthaltenen Kacheln, die er zunächst auch starten kann und die den Kanon seiner Aufgabenwahrnehmung abbilden.

Frontend-Backend-Rollen

- Mit Hilfe des Reports **PRGN_CREATE_FIORI_BACKENDROLES** kann in S/4 HANA aus einer Frontend- eine Backend-Rolle erstellt werden. So haben wir zu jeder im Frontend installierten App eine zugehörige Backend App. Und so werden bei der Definition der Aufgabenrollen die zugehörigen Backend Apps zu den Frontend-Rollen gefunden und zugefügt.
- Wenn die entsprechende App im Backend vorliegt, ist es letztlich wie im ehemaligen PFCG: Die Apps gelten dann als SU24-Vorgabe inkl. zugehörigem Service und werden automatisch herangezogen.

Vorschlagswerte

- In früheren Zeiten wurden die Nutzungsvorgaben im Kundennamensraum selten gepflegt, sodass hier eigentlich immer manuelle Eingriffe notwendig waren. Bei der Nutzung von Fiori Apps ist es somit empfehlenswert, die Berechtigungsvorschläge für SU24 (SU25) immer zu pflegen. Es ist fast zwingend, weil man an dem technischen Aufbau einer Rolle nicht mehr identifizieren kann, welche App mit Service sich dahinter verbirgt.
- Hinzu kommt, dass Fiori Apps auch neu ausgeliefert werden können in einer völlig neuen Version. Und eine neue Version erhält eine neue ID. Also ist es ein neues Element, welches auch neu berechtigt und der Rolle zugewiesen werden muss.

Gefahr der Maximalausprägung

enercity
positive energie

- Der Umstieg im Unternehmen soll üblicherweise schnell und reibungslos vonstattengehen. Da die HANA / Fiori -Umgebung neu ist, möchte man sich kaum mit den alten Rollen und Berechtigungen, vor allem den alten Berechtigungsausprägungen, beschäftigen. In vielen Unternehmen werden üblicherweise gar nicht alle Ausprägungsmöglichkeiten der Steuerungsfelder genutzt, sondern nur **neuralgische** Feldausprägungen als **ausschließlicher Separierer** in den Rollen.
- Wenn nun diese Punkte ebenfalls als Vollausprägung eingestellt / geändert werden, damit alles reibungslos läuft, anstatt neue Rollen hinzuzufügen, laufen die Anwender in hohem Maße auf Fehler, möglicherweise insbesondere auf viel zu hohe Berechtigungen und somit in regelmäßige SoD-Konflikte.
- Die bedeutet besondere Vorsicht bei der Gestaltung.

SU53

- Entsprechend ist hier mit Vorsicht und weitestgehender Neugestaltung zu arbeiten. SU53 (Fehlende Berechtigungen anzeigen) funktioniert natürlich weiterhin. Wenn der Berechtigungsadministrator die SU53 kennt und Benutzer auf Fehler laufen, kann über SU53 zu jedem Benutzer gewechselt werden, um sich die Fehlerinhalte anzeigen zu lassen und dann in einem Folgeschritt die Berechtigungsverursachung zu eliminieren.
- Der Anwender selbst kann dies nicht mehr, die Administration kann jedoch die alten Werkzeuge, die durchaus nicht nur ihre Berechtigung hatten, sondern etabliert hervorragend laufen, weiterhin nutzen. Trace-Nutzungen sind natürlich ebenso möglich.

Möglichkeiten zur Analyse

- Es ist möglich, alte SAP-Funktionen unter HANA zu nutzen, aber dies referenziert natürlich auf die alte Welt. Daher schwierig ! Aber – und insoweit verständlich – gibt es seit ein paar Jahren Reports zum Auswerten, z.B. von Apps in Rollen. Der Report **RSUSR_START_APP** ist hierfür gedacht.
- Unternehmen, die Access Control einsetzen, können Fiori-Apps als Namen eingeben und entsprechend SoD-Konflikte identifizieren. Das ist ein Vorteil, den man aber auch erwarten kann.
- Was wichtig ist, ist das Grundkonzept der Server-Sicherheit (bis zur Betriebssystem [Unix]-Ebene), da man, sofern er nicht im Backend installiert ist, einen zusätzlichen Frontend-Server hat. So wird ein eigenes Sicherheitskonzept für die Kommunikation zwischen Frontend- und Backend-Server benötigt.
- SAP HANA kann jedoch auch als Cloud-Lösung genutzt werden, dort sieht die Frage der Gesamtsicherheit wiederum anders aus.

HANA & Security

- Zusätzlich ist zu beachten, dass HANA eine neue Ebene ist, denn HANA ist kaum allein als Datenbank zu bezeichnen, sondern vielmehr als Applikation zu sehen, die auch Datenbank ist, aber eben auch ein Konzept.
- Dies ist im Security-Bereich bis zum Rollenbau zu beachten, denn es gelten eben bis zum **DBACOCKPIT** (SQL auf Tabellen und Views) unterschiedliche Ebenen der Sicherheit zu beachten, die nun elementar sind und beschrieben werden müssen. Awareness ist grundlegend. Ansonsten können in der HANA Datenbank leicht S/4-Daten geändert werden.
- Zu beachten ist auch das Fahren als Multicontainersystem, im Sec.-Bereich bei mehreren unabhängigen log. DB / Multitenant und differentem SSL analog zu administrieren und zu behandeln.

Wichtige Tabellen und Views

enercity
positive energie

M_CONNECTIONS

M_REMOTE_CONNECTIONS

M_REMOTE_STATEMENTS

M_HOST_INFORMATION

M_ENCRYPTION_OVERVIEW

M_PERSISTENCE_ENCRYPTION_KEYS

M_PERSISTENCE_ENCRYPTION_STATUS

M_INIFILE_CONTENTS

_SYS_SECURITY._SYS_PASSWORD_BLACKLIST

_SYS_REPO.DELIVERY_UNITS

_SYS_REPO.PACKAGE_CATALOG

_SYS_REPO.OBJECT_HISTORY

_SYS_REPOSITORY_REST

SYS.REMOTE_USERS

SYS.USERS

PRIVILEGES

OBJECT_PRIVILEGES

STRUCTURED_PRIVILEGES

GRANTED_ROLES

GRANTED_PRIVILEGES

EFFECTIVE_PRIVILEGES

EFFECTIVE_PRIVILEGES_GRANTED

EFFECTIVE_ROLES

EFFECTIVE_APPLICATION_PRIVILEGES

EFFECTIVE_STRUCTURED_PRIVILEGES

TABLES

SYS.AUDIT_POLICIES

SYS.AUDIT_LOG

Wesentliche Literatur

Tiede, Thomas (2021): Sicherheit und Prüfung von SAP-Systemen: SAP-S/4HANA-Landschaften prüfen und absichern, SAP Press. (ISBN-13: 978-3836277549)

Tiede, Thomas (2019): SAP HANA - Sicherheit und Berechtigungen: Systemsicherheit für Datenbank, SAP S/4HANA und SAP BW/4HANA, SAP Press. (ISBN-13: 978-3836267656)

Brunner et al. (2021): Schnelleinstieg in SAP S/4HANA, Espresso Tutorials. (ISBN-13: 978-3960122753)

Brandeis, Jörg (2020): SQLScript für SAP HANA: Performante Datenbankabfragen für SAP HANA erstellen, SAP Press. (ISBN-13: 978-3836274081)

https://www.wildensee.de

Vielen Dank für
Ihre Aufmerksamkeit!

Christoph Wildensee
Tel.: 0511-430-2128

enercity
positive energie