COGNITUM Software

go:Roles – Die effiziente Lösung für Berechtigungsanalyse und Rollendesign

Profitieren Sie von den Vorteilen einer automatisierten Lösung

Die Situation

Wer hat welche Berechtigung? Warum? Berechtigungen werden auch heutzutage immer noch nach bestem Wissen und Gewissen vergeben.

Selbst die Zuweisung von Berechtigungen im Rahmen einer Identity und Access Governance Lösung erfolgt auf Basis von „weichen" Faktoren.

Ebenso erfolgt die Umsetzung eines rollenbasierten Berechtigungskonzeptes auf Basis bestehender Berechtigungszuordnungen, die unter Umständen seit Jahren gewachsen und nicht immer revisioniert worden sind.

Die Herausforderung

Anforderungen von Geschäftsführung, Datenschutz und Revision

Die Einführung eines rollenbasierten Berechtigungskonzeptes hat Effekte ab dem Zeitpunkt der Einführung. Bestehende Berechtigungen werden entweder nur oberflächlich oder mit sehr hohem zeitlichem und personellem Aufwand in Rollen transformiert. Daher stellt sich die Frage, wie können Standardprozesse der Berechtigungsverwaltung kostengünstig und ohne hohen Aufwand automatisiert werden?

Zusätzlich muss die steigende Zahl regulativer Anforderungen berücksichtigt werden, die eine Transformation der „alten" Berechtigungen in ein Rollenkonzept zwingend notwendig macht.

Rollen – eine Definition

- Rollen sind eine logische Verbindung von Benutzern und Ressourcen. Eine Rolle definiert Aufgaben, Eigenschaften und vor allem Rechte eines Benutzers.
- Eine Rolle beschreibt, warum bestimmte Ressourcen benötigt werden.
- Statt Benutzern Rechte direkt zuzuweisen, wird eine Benutzerrolle definiert, die dann vielen Benutzern zugeordnet werden kann.
- Rollen sind unabhängig von Benutzern modellierbar und definierbar.
- Rollenverwaltung ist unverzichtbar für Governance, Risk Management, Compliance.
- SoD-Regeln (Segregation of Duties) beziehen sich in der Regel auf Funktionen, also auf Rollen.
- Um administrative Effizienz in der Verwaltung von Zugriffsrechten umzusetzen, benötigt man Rollen
  - für die Zertifizierungen von Zugriffsrechten,
  - für die Attestierung von Verantwortlichkeiten.
- Rollen sind die Basis für eine strukturierte Identity und Access Governance.

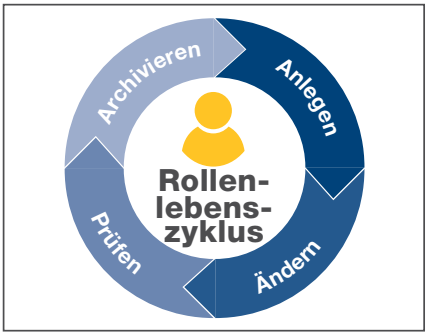
Die Lösung

Eine vollständige, umfassende und zentralisierte Rollenverwaltung

go:Roles ist ein umfassendes Werkzeug für das Design, die Kontrolle und die Pflege von Businessrollen-Modellen im Rahmen einer Identity und Access Governance Lösung (IAG).

Es dient der initialen Berechtigungsanalyse in Vorbereitung einer Rollenmodellierung. Die Rollenmodellierung unterstützt sowohl die Einführung, als auch den fortlaufenden Betrieb einer IAG-Lösung mit rollenbasierender Berechtigungsverwaltung (RBAC). Darüber hinaus liefert **go:Roles** eine Grundlage für eine möglicherweise geforderte Funktionstrennung (Segregation of Duties, SoD).

Dabei ist **go:Roles** unabhängig von vorhandenen IAG-Lösungen einsetzbar. Neben der zentralen, applikationsübergreifenden Analyse und Rollenmodellierung, kann über **go:Roles** sowohl eine dedizierte Analyse einer beliebigen Anwendung hinsichtlich der verwendeten Berechtigungen, als auch der zugewiesenen Benutzerkonten erfolgen.



Auf dieser Basis kann eine nachgelagerte Zertifizierung sowohl von Berechtigungsobjekten (Rollen und Einzelrechte), als auch von Benutzern und den zugewiesenen Berechtigungen einer Anwendung in der vorhandenen IAG-Lösung initiiert werden.

Kernfunktionen

Unterstützung in allen Phasen und Prozessen

- Bei der Datenerhebung für Organisation, Identitäten, Zielsystemkonten und Zielsystemberechtigungen
- Bei der initialen Rollenmodellierung, gestützt durch intelligente Role Mining Methoden
- Bei der Erstbefüllung einer IAG-Lösung (der initialen Ist-Aufnahme von Zielsystemen)
- Bei der anschließenden Pflege des gesamten Rollenmodells
- Bei allen Veränderungen der Organisationsstruktur und der IT-Infrastruktur

User Interface

Intuitives und benutzerfreundliches User Interface

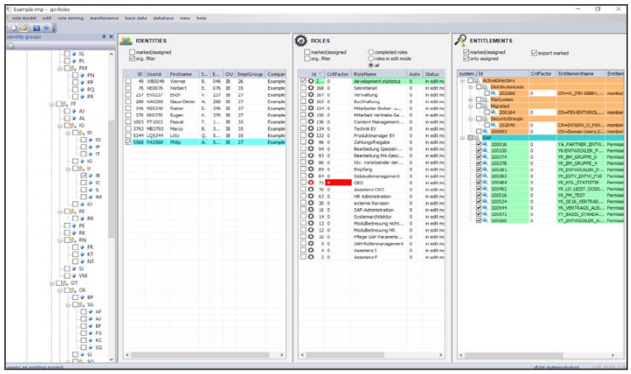


*Abbildung: Hauptfenster von **go:Roles**, unterteilt in Organisationsstruktur, Identitäten, Rollen und Berechtigungen*

- Übersichtliche und performante Darstellung der Beziehungen zwischen Organisation ⇔ Mitarbeiter ⇔ Rollen ⇔ Berechtigungen
- Schnelle Filterung der relevanten Information
- Massenoperationen auf mehreren Rollen
- Vergleichen von Rollen

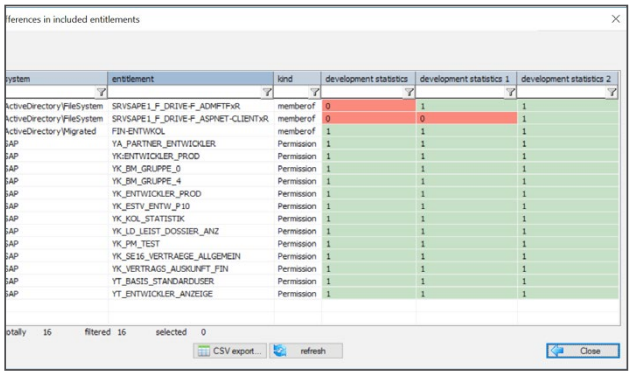


Abbildung: Vergleich von Rollen anhand enthaltener Berechtigungen

- Visualisierung von Rollenunterschieden
- Systemübergreifende Suchfunktion
- Aufgabenorientierte Zugriffsverwaltung
- Listendialoge ermöglichen es, eine Auswahl aus angezeigten Listen zu treffen

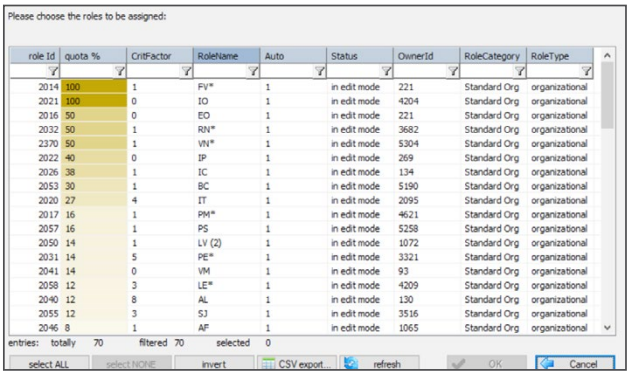
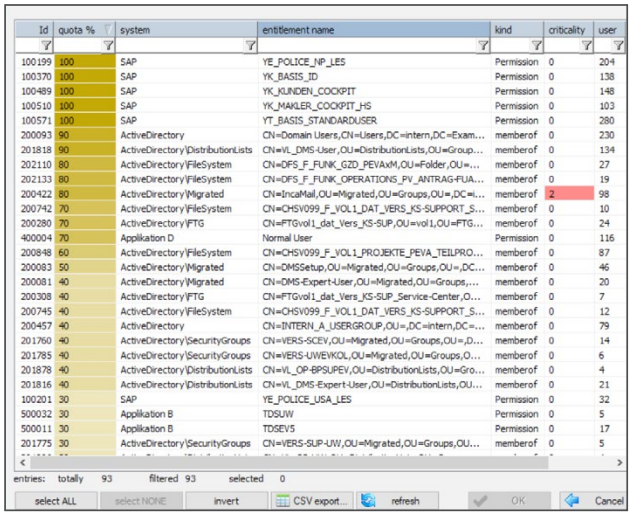


Abbildung: Vorschlag von Rollenzuordnungen

Kontextabhängig können ein oder mehrere Elemente durch Selektion gewählt werden. Die angezeigten Elemente des Listendialogs können gefiltert werden.



Id	quota %	system	entitlement name	kind	criticality	user
100199	100	SAP	YE_POLICE_NP_LES	Permission	0	204
100370	100	SAP	YK_BASIS_ID	Permission	0	138
100489	100	SAP	YK_KUNDEN_COCKPIT	Permission	0	148
100510	100	SAP	YK_MAKLER_COCKPIT_HS	Permission	0	103
100571	100	SAP	YT_BASIS_STANDARDUSER	Permission	0	280
200093	90	ActiveDirectory	CN=Domain Users,CN=Users,DC=intern,DC=Exam…	memberof	0	230
201818	90	ActiveDirectory\DistributionLists	CN=VL_DMS-User,OU=DistributionLists,OU=Group…	memberof	0	134
202110	80	ActiveDirectory\FileSystem	CN=DFS_F_FUNK_GZD_PEVAxM,OU=Folder,OU=…	memberof	0	27
202133	80	ActiveDirectory\FileSystem	CN=DFS_F_FUNK_OPERATIONS_PV_ANTRAG-FUA…	memberof	0	19
200422	80	ActiveDirectory\Migrated	CN=IncaMail,OU=Migrated,OU=Groups,OU=,DC=i…	memberof	2	98
200742	70	ActiveDirectory\FileSystem	CN=CHSV099_F_VOL1_DAT_VERS_KS-SUPPORT_S…	memberof	0	10
200280	70	ActiveDirectory\FTG	CN=FTGvol1_dat_Vers_KS-SUP,OU=vol1,OU=FTG…	memberof	0	24
400004	70	Applikation D	Normal User	Permission	0	116
200848	60	ActiveDirectory\FileSystem	CN=CHSV099_F_VOL1_PROJEKTE_PEVA_TEILPRO…	memberof	0	87
200083	50	ActiveDirectory\Migrated	CN=DMSSetup,OU=Migrated,OU=Groups,OU=,DC…	memberof	0	46
200081	40	ActiveDirectory\Migrated	CN=DMS-Expert-User,OU=Migrated,OU=Groups,…	memberof	0	20
200308	40	ActiveDirectory\FTG	CN=FTGvol1_dat_Vers_KS-SUP_Service-Center,O…	memberof	0	7
200745	40	ActiveDirectory\FileSystem	CN=CHSV099_F_VOL1_DAT_VERS_KS-SUPPORT_S…	memberof	0	12
200457	40	ActiveDirectory	CN=INTERN_A_USERGROUP,OU=,DC=intern,DC=…	memberof	0	79
201760	40	ActiveDirectory\SecurityGroups	CN=VERS-SCEV,OU=Migrated,OU=Groups,OU=,D…	memberof	0	14
201785	40	ActiveDirectory\SecurityGroups	CN=VERS-UWEVKOL,OU=Migrated,OU=Groups,O…	memberof	0	6
201878	40	ActiveDirectory\DistributionLists	CN=VL_OP-BPSUPEV,OU=DistributionLists,OU=Gro…	memberof	0	4
201816	40	ActiveDirectory\DistributionLists	CN=VL_DMS-Expert-User,OU=DistributionLists,OU…	memberof	0	21
100201	30	SAP	YE_POLICE_USA_LES	Permission	0	32
500032	30	Applikation B	TDSUW	Permission	0	5
500011	30	Applikation B	TDSEV5	Permission	0	17
201775	30	ActiveDirectory\SecurityGroups	CN=VERS-SUP-UW,OU=Migrated,OU=Groups,OU…	memberof	0	5

entries: totally 93 filtered 93 selected 0

select ALL | select NONE | invert | CSV export… | refresh | OK | Cancel

Abbildung: Role Mining – Vorschläge für Berechtigungsergänzungen

Rollenmodellierung (Role Mining)

- Freie Auswahl der organisatorischen Faktoren im Rollenmodell
- Vererbungsunterstützung durch hierarchische Rollenmodellierung
- Top-down- und Bottom-up-Methodik
- Bewährte und optimierte Methoden zur Rollenanalyse
- Intelligente Erstellung von Ergänzungsvorschlägen und Kandidatenlisten
- Organisations- und funktionsorientierte Rollenbildung

Role Definition

- Inklusive Regelwerk für eine empfänger- und antragstellerorientierte Rollenzuweisung
- Fachgerechte und praxisorientierte Rollenattribute
- Erstellung von Rollenkatalogen

Berechtigungen und Zuweisungen können aus verschiedenen Zielsystemen konsolidiert eingelesen, analysiert und ausgewertet werden. Ebenso können organisatorische Informationen importiert werden, um diese in Kontext zu den Berechtigungen zu setzen, wodurch man automatisch ein Rollenkonzept vorgeschlagen bekommt, dessen Einflussparameter man justieren kann.

Rollenpflege

- Versionierung der Rollen
- Kennzeichnung des Rollenstatus zur Unterstützung bei Freigabeverfahren
- Archivierung von Rollen
- Ermittlung identischer und ähnlicher Rollendefinitionen hinsichtlich Berechtigungen und Zuordnung von Identitäten
- Ermittlung von Rollen, welche in anderen Rollen enthalten sind
- Ermittlung nicht mehr benötigter Rollen
- Ermittlung spekulativer Rollenzuordnungen

Validierung von Rollen und Zuweisungen

Id	CritFactor	RoleName	Auto	Status	OwnerId	RoleCategory	RoleType	owner	user	Entitlements count	assignments	valid_from	valid_to	created
2…	0	IP	1	in edit mode	269	Standard Org	organiz…	F., Jean, JF0269	3	5	15	22.03.2018	31.12.2999	2018-03-22
2…	0	IJ*	1	in edit mode	5546	Standard Org	organiz…	C., Franck, FC5546	28	5	140	22.03.2018	31.12.2999	2018-03-22
2…	0	IB	1	in edit mode	5568	Standard Org	organiz…	A., Philip, PA5568	10	107	1070	22.03.2018	31.12.2999	2018-03-22
2…	1	IC	1	in edit mode	134	Standard Org	organiz…	O., Dominik, DO0134	6	18	108	22.03.2018	31.12.2999	2018-03-22
2…	0	IL	1	in edit mode	196	Standard Org	organiz…	E., Alfred, AE0196	5	3	15	22.03.2018	31.12.2999	2018-03-22
2…	0	IM	1	in edit mode	5238	Standard Org	organiz…	G., Damien, DG5238	6	8	48	22.03.2018	31.12.2999	2018-03-22
2…	5	PE*	1	in edit mode	3321	Standard Org	organiz…	J., Martin, MJ3321	3	21	63	22.03.2018	31.12.2999	2018-03-22
2…	1	RN*	1	in edit mode	3682	Standard Org	organiz…	K., Roberto, RK3682	14	2	28	22.03.2018	31.12.2999	2018-03-22
2…	0	FR	1	in edit mode	4007	Standard Org	organiz…	X., Reiner, RX4007	3	29	87	22.03.2018	31.12.2999	2018-03-22
2…	0	KT	1	in edit mode	4917	Standard Org	organiz…	V., Christoph, CV4917	4	25	100	22.03.2018	31.12.2999	2018-03-22
2…	0	NT	1	in edit mode	3289	Standard Org	organiz…	B., Sandra, SB3289	6	7	42	22.03.2018	31.12.2999	2018-03-22

Abbildung: Validierung von Rollen und Rollenzuordnungen

- Soll-Ist-Vergleich durch Gegenüberstellung der Rollenzuweisungen (Soll) und der tatsächlichen Berechtigungsvergabe (Ist)
- Vorlagen zur Bereinigung von Berechtigungszuordnungen

Weitere Funktionen

- Übersichtliche und performante Darstellung von Rollenzuweisungen und Berechtigungen
- Fokussierung auf Organisationszweige und -einheiten
- Zweckmäßige Filter- und Sortierfunktionen
- Berücksichtigung von Gültigkeitszeiträumen
- Exportfunktionen, z.B. für Rollendefinitionen

go:Roles Technische Informationen

Die Anwendung basiert auf einer Client-Server-Architektur und ist

- unabhängig von bereits eingesetzten IAG-Lösungen
- Windows- und datenbankbasierend
- Multi-User-fähig
- Auto-Update-fähig
- mehrsprachig (DE, EN)

go:Roles Workshop

Für den Einsatz von **go:Roles** wird ein begleitender Workshop angeboten, um den besten Nutzen und optimale Ergebnisse erzielen zu können:

- Schritt 1: Rollenkonzept, Festlegung von Ziel und Verfahren
- Schritt 2: Entwicklung der Rollenmodell-Basis
- Schritt 3: Datenerhebung, Datenintegration, Datenbereinigung
- Schritt 4: Ermittlung von Rollenkandidaten
- Schritt 5: Definition und Zertifizierung von Rollen
- Schritt 6: Realisierung
- Schritt 7: Rollen-Management

go:Roles Workshop Methodik

- Denken Sie im Ganzen, aber starten Sie klein.
- Kombinieren Sie den Top-Down und den Bottom-Up Ansatz: Welche Rollen benötigt das Business (Top-Down) und welche Rollen ergeben sich aus den Privilegien der User (Bottom-Up)?
- Rollen und Rollenmodelle sind mehrstufig und hierarchisch.
- Rollen erlauben Ihnen mehr Flexibilität. Nutzen Sie diese und hinterfragen Sie regelmäßig Ihr Rollenmodell.
- Rollen sollen wiederverwendet werden können.
- Wer ist wofür zuständig? Nur mit einer klaren Regelung, wer für welche Rollen verantwortlich ist, lässt sich ein Rollenmodell langfristig umsetzen.
- Arbeiten Sie immer mit aktuellen und vor allem validen Daten. Dazu gehört, die Ziel- und Quellsysteme aufzuräumen und zu bereinigen.
- Business und IT müssen das Projekt gemeinsam treiben, nur so kommen Sie auch ans Ziel!

go:Roles

Profitieren Sie von den Vorteilen einer automatisierten Lösung

- ✓ **go:efficient** – Vermeidung von Personaleinsatz
- ✓ **go:cost-effective** – Schnelle Ergebnisse
- ✓ **go:simple** – Auflösung von Berechtigungskomplexität
- ✓ **go:integrative** – Integrierbar mit jeder IAG Lösung

COGNITUM Software

go:Roles

COGNITUM Software bündelt langjährige Identity und Access Governance Expertise für die Entwicklung von Standardsoftware.

Identity & Access Governance ist eine Kernkomponente im Aufbau einer sicheren IT-Infrastruktur. Mit unserer umfangreichen Praxiserfahrung aus der Beratung, Implementierung und unserem Know-how für Identity und Access Governance Lösungen haben wir unsere Produkte entwickelt, die schnell und kostensparend für jedes Unternehmen – unabhängig von der Branche und Größe – einsetzbar sind. COGNITUM Software gehört zur ITConcepts Unternehmensgruppe, einem weltweit operierenden IT-Dienstleister und Systemintegrator.

COGNITUM Software GmbH
In den Dauen 6, 53117 Bonn, Deutschland • Tel.: +49 228 9087330 • E-Mail: goidentity@cognitum-software.com • Web: cognitum-software.com