

Kernsystem Verkehrsrechnerzentralen

Tutorial Zugriffsrechte Datenverteiler

Ersteller:



Autor:

PID:

Version: 2.0 Stand 03.06.2019 Status: akzeptiert LBNW14.019-2.0

Submodell:----Dokument:LBNW14.019 Zugriffsrechte-Tutorial-2.0.doc VS-Einstufung: ----

Projekt ID AG: ____ Projekt ID AN: LBNW14.019 Tutorial Zugriffsrechte

Kappich Systemberatung

Im Auftrag des Landesbetriebs Straßenbau NRW



1 Allgemeines

Verteilerliste

Entfällt. Dokumentverteilung entsprechend aktuellem Projektverteiler.

Versionsübersicht

Nr.	Datum	Version	Änderungsgrund	Bearbeiter
1	08.04.11	0.1	Ersterstellung	Westermann
2	28.06.11	1.0	Überführung in den Zustand akzeptiert	Westermann
3	05.09.16	1.1	Berücksichtigung der aktuellen Datenmodelle	Westermann
4	03.06.19	2.0	Berücksichtigung der aktuellen Kernsoftware 3.13	Westermann

Tabelle 1-1: Versionsübersicht

Änderungsübersicht

Nr.	Version	geändertes Kapitel	Beschreibung der Änderung
1	0.1	alle	Ersterstellung
2	1.0	alle	Korrekturen interne QS (Kappich)
3	1.1	2.1, 2.2, 3	Datenmodell Zugriffsrechte (neu) angepasst
4	2.0	alle	Berücksichtigung der aktuellen Kernsoftware 3.13

Tabelle 1-2: Änderungsübersicht

Kurzbeschreibung

In diesem Dokument wird beschrieben, wie für bestehende Systeme die neuen Zugriffsrechte eingestellt werden können. Dazu wird der Anwender durch die Beschreibung des Workflows und wichtiger Zusammenhänge unterstützt.



Inhalt

1	Allgemeines	2
	Verteilerliste	2
	Versionsübersicht	2
	Änderungsübersicht	2
	Kurzbeschreibung	2
	Inhalt	3
	Abkürzungen	5
	Definitionen	5
	Verzeichnis der Tabellen	5
	Verzeichnis der Abbildungen	5
	Referenzierte Dokumente	6
2	Zugriffsrechteprüfung durch den Datenverteiler	7
	2.1 Benutzer	8
	2.2 Berechtigungsklasse	8
	2.2.1 Rolle	8
	2.2.1.1 Attributliste AktivitätDaten[0]	9
	2.2.1.2 Attributliste AktivitätMongop[0,]	10
	2.2.1.3 Attributiste Aktivitativengen[0]	11
	2.2.1.5 Beispiel für die Ermittlung der resultierenden Aktivitäten	11
	2.2.2 Region	14
	2.2.2.1 EnthalteneObjekte[0]	15
	2.2.2.2 AusgeschlosseneObjekte[U] 2.2.2.3 Überlagerung der Regionen	16 16
	2.2.3 Parametrierung der Berechtigungsklassen	17
	2.2.3.1 Rolle / Regionen - Paar	17
	2.2.3.2 Überlagerung Rolle / Regionen - Paare	19
	2.3 Festlegung der Benutzerrechte	20
3	Einstellung der Zugriffsrechte für ein fiktives Teilsystem	21
	3.1 Grundsätzliche Fragestellungen	22
	3.2 Beispiel UZ Schwelm	23
	3.2.1 Versorgung für die Zugriffsrechte relevanten Konfigurationsobjekte	23
	3.2.2 Kurzbeschreibung der Aufrufparameter (Kernsoftware)	25
	3.2.3 Kontrolle der Parametrierung (Erststart)	28
	3.2.3.1 Benutzer	30
	3.2.3.2 Berechtigungsklassen	32

Tutorial Zugriffsrechte Datenverteiler Allgemeines

Kappich Systemberatung integrativ und unabhängig Kompetenz in System- und Verkehrstechnik

3.2.3.3	B Rollen	33
3.2.3.4	Region	30
3.2.4	Einschaltung der Zugriffsrechteprüfung	38
3.2.5	Darstellung der Rechte mit dem GTM	44
3.3 Kop	pplung zweier Datenverteilersysteme	45
3.3.1	Konfiguration der Datenverteilerverbindung	47
3.3.1.1	UZ Ennepetal	47
3.3.1.2	2 UZ Schwelm	48
3.3.2	Start der Systeme	53
3.3.3	Einstellung der Zugriffsrechte zwischen Datenverteilern	54
3.3.4	Beispiel	55



2

2

Abkürzungen

siehe Dokument "Abkürzungen".

Definitionen

siehe Dokument "Glossar".

Verzeichnis der Tabellen

Tabelle 1-1: Versionsübersicht Tabelle 1-2: Änderungsübersicht

Verzeichnis der Abbildungen

Abbildung 2-1: Datenmodell Zugriffsrechte	7
Abbildung 2-2: Attributgruppe Aktivitäten	8
Abbildung 2-3: Überlagerung AktivitätDaten	12
Abbildung 2-4: Überlagerung Rollen	13
Abbildung 2-5: Überlagerung Aktivitäten (Gesamtergebnis)	14
Abbildung 2-6: Attributgruppe Region	14
Abbildung 2-7: Überlagerung Region	17
Abbildung 2-8: Rolle / Regionen Paar	17
Abbildung 2-9: Beispiele Rolle / Regionen Paare	18
Abbildung 2-10: Überlagerung von Rolle / Regionen Paaren	19
Abbildung 2-11: Überlagerung Berechtigungsklassen	20
Abbildung 3-1: Beispiel Unterzentrale	21
Abbildung 3-2: Erforderliche Objekte für die Zugriffsrechte	22
Abbildung 3-1: Datei passwd	26
Abbildung 3-2: Beispiel Datei benutzerverwaltung.xml	27
Abbildung 3-3: Parametrierung der Parametrierung (Erster Start)	28
Abbildung 3-4: Parametrierung der Parametrierung	29
Abbildung 3-5: Parametrierung der Benutzer	30
Abbildung 3-6: Parametrierung des Benutzers Westermann (Berechtigungsklassen)	30
Abbildung 3-7: Kontrolle der Benutzerparameter	31
Abbildung 3-8: Benutzerparameter nach Durchführung der Parametrierung	31
Abbildung 3-9: Parametrierung der Berechtigungsklassen	32
Abbildung 3-10: Parametrierung der Zugriffsrollen	33
Abbildung 3-11: Parametrierung der Zugriffsrollen (Übersicht)	33
Abbildung 3-12: Parametrierung der Zugriffsrolle Adminstratoren	34
Abbildung 3-13: Parametrierung der Zugriffsrolle Operator	35
Abbildung 3-14: Parametrierung der Regionen	36
Abbildung 3-15: Parametrierung der Region Gesamt	37
Abbildung 3-16: GTM als Beobachter starten	38
Abbildung 3-17: Anmeldung Empfänger StörfallZustand (als Beobachter)	39
Abbildung 3-18: Anmeldung Quelle StörfallZustand (als Beobachter)	39
Abbildung 3-19: GTM als Administrator starten	40
Abbildung 3-20: Anmeldung Quelle StörfallZustand (als Administrator)	40
Abbildung 3-21: Onlinetabelle StörfallZustand (als Beobachter)	41
Abbildung 3-22: Änderung der Aktivitäten zur Rolle Bebachter (als Administrator)	42

Systemberatung
integrativ und unabhängig
Kompetenz in System- und Verkehrstechnik

Abbildung 3-23: Onlinetabelle StörfallZustand entzogene Rechte (als Beobachter)	43
Abbildung 3-24: Onlinetabelle StörfallZustand (wieder) erteilte Rechte (als Beobachter)	43
Abbildung 3-25: GTM Menü Ansicht	44
Abbildung 3-26: Onlinetabelle StörfallZustand (als Beobachter)	44
Abbildung 3-27: Kopplung zweier Datenverteilersysteme	45
Abbildung 3-28: Datenverteilerverbindungsobjekt	46
Abbildung 3-29: Kopplung zweier Datenverteilersysteme	46
Abbildung 3-30: Versorgung Datenverteiler dav.uz.ennepetal	47
Abbildung 3-31: Versorgung Benutzer uz.ennepetal.benutzer.uz.schwelm	47
Abbildung 3-32: Benutzerverwaltung UZ Ennepetal (Auszug Datei benutzerverwaltung.xml)	47
Abbildung 3-33: Auszug passwd UZ Schwelm	48
Abbildung 3-34: Versorgung Datenverteiler dav.uz.schwelm	48
Abbildung 3-35: Versorgung Datenverteilerverbindung davDaV.uz.schwelm.uz.ennepetal	49
Abbildung 3-36: Versorgung Benutzer uz.schwelm.benutzer.uz.ennepetal	49
Abbildung 3-37: Parametrierung Benutzer "EnnepetalRechteInSchwelm"	50
Abbildung 3-38: Parametrierung Berechtigungsklasse "EnnepetalRechteInSchwelm"	50
Abbildung 3-39: Parametrierung Aktivitäten "EnnepetalRechteInSchwelm"	51
Abbildung 3-40: Parametrierung Region EnnepetalRechteInSchwelm	52
Abbildung 3-41: Beispielszenario Datenverteilerverbindung	54
Abbildung 3-42: Anmeldung bei der UZ Ennepetal auf Daten der UZ Schwelm	55
Abbildung 3-43: Daten zu den MQ der UZ Schwelm für Benutzer X	56
Abbildung 3-44: Einschränkung der Zugriffsrechte für Ennepetal auf Daten in Schwelm	57
Abbildung 3-45: Auswirkung der Einschränkung für Benutzer X	58
Abbildung 3-46: Auswirkung Rücknahme der Einschränkung für Benutzer X	58

Referenzierte Dokumente

[BetrInf_KS]	Betriebsinformationen der Kernsoftware, aktueller Stand
[BetrInf_Param]	Betriebsinformation Segment 8 (PuK), SWE 8.2 Parametrierung, aktueller Stand



2 Zugriffsrechteprüfung durch den Datenverteiler

Die Prüfung der Zugriffsrechte erfolgt über den Datenverteiler. Dabei wird für den Benutzer, der Daten empfangen oder senden will, geprüft, ob die notwendigen Rechte vorliegen.

Abbildung 2-1 skizziert das Datenmodell zur Beschreibung der (neuen) Zugriffsrechte für einen Benutzer, der sich beim Datenverteilersystem angemeldet:



 KV[0..]
 KB[0..]
 Typ[0..]
 Menge
 Region[0..]
 Typ[0..]
 Menge

 KB:
 Abkürzung für Konfigurationsbereich
 Abkürzung für Konfigurationsbereich
 Abkürzung für Konfigurationsbereich

KV: Abkürzung für Konfigurationsverantwortlicher

Menge: Abkürzung für Mengenbezeichnung

Abbildung 2-1: Datenmodell Zugriffsrechte

Ein Benutzer bildet im Datenmodell eine Person ab, unter dem sich eine Applikation beim Start gegenüber dem Datenverteiler authentifizieren muss. Dabei kann es sich bei der Applikation um die Bedienung und Visualisierung (BuV) oder z.B. den Generischen Testmonitor (GTM) handeln, an der sich ein Mensch über den Login-Dialog anmeldet. Es kann sich genauso um eine Systemapplikation handeln, die auf dem Verkehrsrechner gestartet wird (z.B. die Datenaufbereitung (DUA) oder das Archiv (Ars).

Über Berechtigungsklassen können verschiedene Benutzer zu einer Gruppe zusammengefasst werden. Dabei können einem Benutzer mehrere Berechtigungsklassen zugeordnet werden.

Die Berechtigungsklassen werden durch Rollen/Regionen Paare definiert. Dabei wird durch die Rolle ausgedrückt, was die Person für Aktivitäten durchführen darf (z.B. bestimmte Daten lesen) und durch die Region, für welche Objekte diese Aktivitäten durchgeführt werden können (z.B. bestimmte Querschnitte).

Objekt[

Menge



In den folgenden Unterpunkten wird detailliert auf die einzelnen Bestandteile des Datenmodells eingegangen.

2.1 Benutzer

Ein Benutzer ist ein dynamisches Objekt, unter dem sich eine Applikation gegenüber dem Datenverteiler authentifiziert. Bei der Applikation kann es sich um einen Prozess handeln, der auf dem Verkehrsrechner läuft (z.B. die Datenaufbereitung) oder es kann sich z.B. um die Bedienung und Visualisierung handeln. In allen Fällen prüft der Datenverteiler (bei eingeschalteter Rechteprüfung) ob der Benutzer, unter dem die Applikation gestartet wurde, berechtigt ist, die über die Datenverteilerschnittstelle eingeleitete Aktion durchzuführen. Dies kann z.B. das Anmelden von Onlinedaten zu bestimmten Konfigurationsobjekten sein, oder die Erzeugung eines neuen dynamischen Objektes z.B. eines neuen Benutzers.

Welche Berechtigungen ein Benutzer hat, wird durch die Zuordnung von Berechtigungsklassen festgelegt.

Die Berechtigungsklassen werden bei den (neuen) Zugriffsrechten durch Parametrierung der Attributgruppe Berechtigungsklassen festgelegt.

2.2 Berechtigungsklasse

Über Berechtigungsklassen können die Rechte verschiedener Benutzer bzw. Benutzertypen zusammengefasst werden.

Berechtigungsklassen sind als Konfigurationsobjekte¹ versorgt. Sie fassen ihrerseits Rollen und Regionen paarweise zusammen.

2.2.1 Rolle

Über eine Rolle² wird festgelegt, welche Aktivitäten ein Benutzer, dem diese Rolle zugewiesen wurde, durchführen darf.

Welche Aktivitäten mit den entsprechenden Rollen durchgeführt werden dürfen, ist parametrierbar. Dazu steht die Parameterattributgruppe Aktivitäten zur Verfügung:

Aktivitäten								
AktivitätDaten[0]								Rollof 1
Name KB[0] Attributgruppe[0] Aspekt[0] Empfänger Sender Quelle Senke								e Kolle[]
AktivitätObjekte[0] AktivitätMengen[0]								
Objek	Objekttyp[0] KB[0] ObjekteErzeugenÄndernLöschen Mengentyp[0] KB[0] Me						MengeÄndern	

Abbildung 2-2:	Attributgruppe	Aktivitäten
----------------	----------------	-------------

Der Datenverteiler prüft ab Version 3.13 bei aktivierter neuer Zugriffsrechteprüfung zusätzlich zu den Onlineberechtigungen die Berechtigung des Benutzers welche Archivanfragen durchgeführt werden können. Dabei werden nur Archivanfragen erlaubt, wenn der Benutzer die entsprechende Berechtigung hat diese Daten auch online als Empfänger anzumelden.

Die Aktivitäten werden über drei Attributlisten beschrieben:

¹ Bei den neuen Zugriffsrechten werden hier entsprechende Konfigurationsobjekte vom Typ typ.berechtigungsklasseNeu versorgt.

² Bei den neuen Zugriffsrechten werden hier entsprechende Konfigurationsobjekte vom Typ typ.zugriffsRolleNeu versorgt.



2.2.1.1 Attributliste AktivitätDaten[0..]

Mit dieser Attributliste wird spezifiziert, wie die Zugriffrechte beim Datenaustausch für die entsprechende Rolle gesetzt sind. Es wird festgelegt, zu welchen Attributgruppen unter welchen Aspekten grundsätzlich Datensätze empfangen bzw. gesendet werden dürfen. Zu welchen Objekten diese Daten ausgetauscht werden dürfen, ergibt sich durch die zugehörige Region.

Die Attributliste ist als Feld ausgelegt und hat folgende Struktur:

Name

Beschreibender Name dieser Aktivität

• KB[0..]

Array von Konfigurationsbereichen (Referenzen auf Konfigurationsbereiche), die die Auswahl der Attributgruppen filtern.

Wenn dieses Array leer ist, sind alle Attributgruppen ausgewählt

• Attributgruppe[0..]

Array von Attributgruppen (Referenzen auf Attributgruppen). Wenn dieses Array leer ist, sind alle Attributgruppen ausgewählt

• Aspekte[0..]

Array von Aspekten (Referenzen auf Aspekte). Wenn dieses Array leer ist, sind alle Aspekte ausgewählt

Die Möglichkeiten einer Aktivität beziehen sich auf alle laut Konfiguration vorgesehenen Attributgruppen/Aspekt-Kombinationen, die sich aus dem Kreuzprodukt der beiden Arrays ergeben. Laut Konfiguration seien die Attributgruppe A1 mit den Aspekten S1, S2 und S3, die Attributgruppe A2 mit den Aspekten S1, S4 und S5 und die Attributgruppe A3 mit den Aspekten S1 und S6 möglich. Damit ergibt sich durch die Spezifikation Attributgruppe[] und Aspekt[S1] die Auswahl A1/S1, A2/S1 und A3/S1.

• Datenbefugnisse

Über die folgenden Vorgaben wird bestimmt, welche Aktionen ein Benutzer mit den resultierenden Attributgruppen/Aspekt-Kombinationen durchführen kann:

• Empfänger

Gibt an, ob die Daten mit diesen Rechten empfangen (gelesen) werden dürfen.

Sender

Gibt an, ob die Daten mit diesen Rechten gesendet (geschrieben) werden dürfen.

Quelle

Gibt an, ob die Daten mit diesen Rechten als Quelle angemeldet werden dürfen.

Senke

Gibt an, ob die Daten mit diesen Rechten als Senke angemeldet werden dürfen.

Bei den oben genannten Attributen sind als Werte jeweils "ja", "nein" und "keine Aussage" möglich.

Durch den Aufbau der Attributgruppe und dadurch, dass bei einer Berechtigungsklasse mehrere Rollen/Regionen-Paare vorgegeben werden können, ist eine Überlagerung widersprüchlicher Vorgaben möglich, die durch eine Prioritätenvorgabe geregelt werden muss.



Die Prioritätenreihung ist, wie folgt:

- Wenn zu einer Attributgruppen/Aspekt-Kombination nach Auswertung der Parameter keine Aussage zu den Rechten vorliegt (d.h. diese Kombination wurde nicht parametriert) bedeutet dies keine Rechte (implizites Nein):
 "Empfänger": "nein"; "Sender": "nein"; "Quelle": nein; "Senke": nein
- Bei der Überlagerung gilt folgende aufsteigende Priorität: implizites Nein keine Aussage Ja Nein Ein Explizites Nein hat die höchste Priorität und kann nicht mehr aufgehoben werden.

2.2.1.2 Attributliste AktivitätObjekte[0..]

Mit dieser Attributliste wird spezifiziert, welche Objekte neu angelegt, geändert oder gelöscht werden dürfen.³

Die Attributliste ist als Feld ausgelegt und hat folgende Struktur:

• Objekttyp[0..]

Objekttypen, die hier betrachtet werden sollen. Wenn das Array leer ist, sind alle Objekttypen gemeint⁴.

• Konfigurationsbereich[0..]

Konfigurationsbereiche, in denen Objekte neu erzeugt, geändert oder gelöscht werden dürfen. Wenn das Array leer ist, dürfen in allen möglichen Konfigurationsbereichen (grundsätzlich dürfen nur KB geändert werden, für die die entsprechende Konfiguration auch Konfigurationsverantworlicher ist) Objekt erzeugt werden.

ObjekteErzeugenÄndernLöschen

Gibt an, ob zu den spezifizierten Objekttypen, Objekte erzeugt, geändert oder gelöscht werden dürfen.

Bei diesem Attribut kann "Ja" oder "Nein" als Wert angegeben werden. Bei widersprüchlichen Angaben hat "Nein" die höhere Priorität.

³ Diese Zugriffsrechteprüfung wird seit der Version 3.13 der Kernsoftware bei aktivierter neuer Rechteprüfung durchgeführt. Sie ist ab Version 3.13 fest im Datenverteiler integriert (war vorher teilweise als Prototyp durch ein Rechteprüfungs-PlugIn implementiert).

⁴ In Version 3.13 müssen hier noch typ.dynamischesObjekt und ggf. typ.konfigurationsObjekt angegeben werden, um alle Objekte auszuwählen. In folgenden Versionen der Kernsoftware bewirkt ein leeres Array die Wildcard-Auswahl aller Typen.



2.2.1.3 Attributliste AktivitätMengen[0..]

Mit dieser Attributliste wird spezifiziert, welche Mengen geändert werden dürfen.³

Mengentyp[0..]

Mengen, die hier betrachtet werden sollen. Wenn das Array leer ist, sind alle Mengentypen gemeint.

Konfigurationsbereich[0..]

Konfigurationsbereiche, in denen Mengen der angegebenen Mengentypen geändert werden dürfen. Wenn das Array leer ist, dürfen in allen möglichen Konfigurationsbereichen (grundsätzlich dürfen nur KB geändert werden, für die die entsprechende Konfiguration auch Konfigurationsverantworlicher ist) Mengen der angegebenen Mengentypen geändert werden.

• MengeÄndern[0..]

Gibt an, ob zu den spezifizierten Mengentypen Mengen geändert werden dürfen. Bei diesem Attribut kann "Ja" oder "Nein" als Wert angegeben werden. Bei widersprüchlichen Angaben hat "Nein" die höhere Priorität.

2.2.1.4 Attribut Rolle[0..]

Über die optionale Angabe von ein oder mehreren Rolle können Rollen andere Rollen enthalten. Damit ist es möglich, die Rollen hierarchisch zu gestalten.

Bei der Überlagerung von mehreren Rollen werden die Rechte positiv vereinigt. Das bedeutet, wenn eine Rolle eine Aktivität erlaubt und eine andere Rolle diese Aktivität verbietet, ergibt sich als Resultat, dass die entsprechende Aktivität erlaubt ist. Diese Vorgehensweise ergibt sich aus der Anforderung, Rollen hierarchisch aufeinander aufzubauen. Die Rollen A, B, und C beschreiben verschiedene Aktivitäten, wobei die Rolle C mehr Befugnisse ermöglicht als die Rolle B und diese wiederum mehr Befugnisse ermöglicht als die Rolle A. Wenn eine Rolle D die drei Rollen vereinigen soll, dürfen eventuell spezifizierte Verbote der Rolle A nicht Befugnisse der Rolle B oder C überschreiben.

2.2.1.5 Beispiel für die Ermittlung der resultierenden Aktivitäten

Bei dem Beispiel werden ohne Beschränkung der Allgemeinheit die Aktivitäten aus der Attributliste AktivitätDaten[0..] und dem Attribut Rolle[0..] überlagert.

Aktivitäten									
AktivitätDaten[0]								Rollof 1	
Name	Name KB[0] Attributgruppe[0] Aspekt[0] Empfänger Sender Quelle Senke								e Kone[]
AktivitätObjekte[0] AktivitätMengen[0]									
Objekttyp[0] KB[0] ObjekteErzeugenÄndernLöschen Mengentyp[0] KB[0]						KB[0]	MengeÄndern		

Über die Attributliste AktivitätDaten[] lassen sich atomare Aktivitäten definieren. Diese atomaren Aktivitäten werden im Folgenden auch Aktionen genannt.



Eine Aktion beschreibt die kleinste unterscheidbare Aktivität, die ein entsprechender Benutzer für ein bestimmtes Objekt durchführen darf oder nicht. Als Beispiel könnten folgende Aktionen beschrieben sein:

- A Verkehrsdaten (Kurzzeit) unter dem Aspekt Analyse als Empfänger anmelden⁵.
- B Verkehrsdaten (Kurzzeit) unter dem Aspekt Analyse als Quelle anmelden.
- C Verkehrsdaten (Kurzzeit) unter dem Aspekt Analyse als Sender anmelden.
- D Verkehrsdaten (Kurzzeit) unter dem Aspekt Analyse als Senke anmelden.
- E Verkehrsdaten (Kurzzeit) unter dem Aspekt Aggregation 1 Minute als Empfänger anmelden.

Die Aktion A 1 kann beispielsweise folgendermaßen spezifiziert sein:

- Name: A
- Attributgruppe: atg.verkehrsDatenKurzZeitMq
- Aspekt: asp.analyse
- Empfänger Ja
- Sender: Keine Aussage
- Quelle: Keine Aussage
- Senke: Keine Aussage

Das folgende Beispiel soll zeigen, wie die Ermittlung der resultierenden Aktivitäten einer Rolle durchgeführt wird.

Abbildung 2-3 skizziert die Parametrierung der Attributliste AktivitätDaten[]. Auf der Ordinate sind die Feldindices der Attributliste aufgeführt. Auf der Abszisse sind die atomaren Aktivitäten aufgeführt, zu denen eine Aussage getroffen wurde.

In dem Beispiel wurden für die Attributliste 3 Feldeinträge gemacht. In Eintrag 1 wurde zu den Aktivitäten A 2 und A 3 keine Aussage gemacht und die Aktivität A 5 wurde erlaubt. In Eintrag 2 wurde die Aktivität A 1 erlaubt, A 2 und A 5 verboten sowie zu A 4 keine Aussage gemacht. Eintrag 3 erlaubt die Aktivitäten A 1 und A 2, verbietet A 5 und macht zu A 3 und A 4 keine Aussage.



Abbildung 2-3: Überlagerung AktivitätDaten

Das Ergebnis der Überlagerung der Feldeinträge zur Attributliste AktivitätDaten[] ist als $\Sigma 1$ gekennzeichnet. Sobald ein Eintrag eine Aktivität als verboten definiert, ist das Resultat verboten. Erlaubt sind die Aktivitäten, zu denen mindestens ein Eintrag erlaubt vorgibt und kein Eintrag diese Aktivität verbietet. Einträge "keine Aussage" haben eine niedrigere Priorität und beeinflus-

⁵ Technisch bedeutet dies, dass eine Applikation z.B. die Bedienung Datensätze zu der Attributgruppe atg.erkehrsDatenKurzZeitMq unter dem Aspekt asp.analyse als einfacher Empfänger unter dem Benutzer angemeldet hat. Damit werden die Daten abonniert und können z.B. in einem Onlineprotokoll dargestellt werden.



sen verbotene oder erlaubte Aktivitäten nicht. Als Resultat ist also A 1 erlaubt, A 2 und A 5 verboten (weil hier jeweils mindestens ein Eintrag die entsprechende Aktivität verboten hatte) und zu A 3 und A 4 wurde resultierend noch keine Aussage gemacht.

Abbildung 2-4 skizziert die Parametrierung des Feldes Rolle[].

Auf der Ordinate sind die Feldindices der Rollen aufgeführt. Auf der Abszisse sind die atomaren Aktivitäten aufgeführt, zu denen eine Aussage getroffen wurde.

In dem Beispiel wurden 3 Rollen in dem Feld angegeben. In Eintrag 1 wurden die Aktivitäten A 2 und A 3 erlaubt. In Eintrag 2 wurde die Aktivität A 1 erlaubt sowie A 2 und A 5 verboten. Eintrag 3 erlaubt die Aktivitäten A 1 und A 2 und verbietet A 3 und A 5.



Abbildung 2-4: Überlagerung Rollen

Bei der Überlagerung der Rollen wird eine Vereinigung der erlaubten Aktivitäten vollzogen. Sobald eine Rolle eine bestimmte Aktivität erlaubt, ist diese Aktivität erlaubt. Als Resultat Σ 2 ergibt sich dementsprechend, dass die Aktivitäten A 1, A 2 und A 3 erlaubt sind. Aktivität A 5 ist verboten.

Für das Gesamtergebnis müssen die beiden Teilergebnisse $\Sigma 1$ und $\Sigma 2$ noch überlagert werden. Bei dieser Überlagerung hat die Parametrierung der Attributliste AktivitätDaten[] Vorrang. Man betrachte hierzu den Anwendungsfall, dass sich die Aktivitäten einer Rolle durch die Aggregation mehrerer Rollen ergeben und zusätzlich vorgegeben werden soll, dass bestimmte Aktivitäten erlaubt oder verboten sein sollen.

Das Gesamtergebnis der Überlagerung ist in Abbildung 2-5 gezeigt. Wie zu sehen ist, setzt sich immer die Vorgabe aus der Parametrierung der Attributliste AktivitätDaten[] durch (siehe A 1, A 2, A 5 und A *j*). Nur für den Fall, dass für bestimmte Aktivitäten keine Aussage getroffen wurde, wird das Ergebnis aus der Überlagerung der Rollen betrachtet (siehe A 3). Wenn zu einer Aktivität keine Aussage getroffen wurde und die Auswertung der Rollen ebenfalls keine Aussage getroffen was ge ergibt, wird die entsprechende Aktivität als verboten betrachtet (siehe A 4).





Abbildung 2-5: Überlagerung Aktivitäten (Gesamtergebnis)

2.2.2 Region

Durch die Region wird spezifiziert, für welche Objekte die Aktivitäten der entsprechenden Rolle aus dem Rolle/Regionen-Paar durchgeführt werden können (z.B. für bestimmte Querschnitte).

Der Parameter enthält zwei Attributlisten, über die spezifiziert werden kann, welche Objekte zu der Region gehören und welche gegebenenfalls ausgeschlossen sind. Die Listen sind gleich aufgebaut und durch weitere Attributlisten strukturiert:

Region										
EnthalteneObjekte[0]										
Bereich	Bereich[0] Region[0] Objekte[0]									
KV[0] KB[0] Typ[0] Menge Region[0] Typ[0] Menge Objekt[0] Me							Menge			
Ausges	AusgeschlosseneObjekte[0]									
Bereich	Bereich[0] Region[0] Objekte[0]									
KV[0]	KB[0]	Typ[0]	Menge	Region[0]	Typ[0]	Menge	Objekt[]	Menge		

Abbildung 2-6: Attributgruppe Region



2.2.2.1 EnthalteneObjekte[0..]

Über diese Vorgaben werden die in der Region enthaltenen Objekte spezifiziert. Die Vorgabe kann über Bereiche, Regionen und einzelne Objekte parametriert werden.

• Bereich[0..]

Auswahl von Objekten über Bereiche.

Attributliste als Årray der Größe 0 bis unbegrenzt. Wenn dieses Array leer ist, erfolgt (hierüber) keine Auswahl von Konfigurationsobjekten.

• Konfigurationsverantwortlicher[0..]

Über dieses Array können Konfigurationsverantwortliche angegeben werden. Die Auswahl eines Konfigurationsverantwortlichen bedeutet, dass alle Konfigurationsbereiche dieses Konfigurationsverantwortlichen betrachtet werden. Wenn das Array Konfigurationsverantwortliche leer ist, ist kein Konfigurationsverantwortlicher und damit kein Konfigurationsbereich ausgewählt.

• Typ[0..]

Über dieses Array werden die bisher ausgewählten Objekte auf die angegebenen Typobjekte beschränkt. Wenn die Arrays Konfigurationsverantwortliche und Konfigurationsbereiche beide zu keiner (Vor)Auswahl von Konfigurationsbereichen geführt haben, wird an dieser Stelle die gesamte Konfiguration betrachtet. D.h., wenn hier z.B. als Typ Mess-Querschnitt angegeben wird, werden nur noch Konfigurationsobjekte betrachtet, die von diesem Typ stammen. Wenn das Array Typen leer ist, erfolgt keine Filterung nach Objekttypen. Damit sind alle bisher ausgewählten Konfigurationsobjekte ausgewählt (Also entweder alle Konfigurationsobjekte der (vor)ausgewählten Bereiche oder alle Konfigurationsobjekte der Konfiguration).

Mengenbezeichnung

Über die Vorgabe eines Mengennamens können die Objekte ausgewählt werden, die in Mengen dieses Namens bei den ausgewählten Objekten enthalten sind. Ist hier z.B. als Menge "FahrStreifen" angegeben, wird für alle bisher ausgewählten Objekte geprüft, ob an dem Konfigurationsobjekt eine Menge dieses Namens vorhanden ist und für diesen Fall werden die enthaltenen Konfigurationsobjekte betrachtet. Wenn hier keine Angabe erfolgt, bleibt die Auswahl bestehen.

• Region[0..]

Auswahl von Objekten über Regionen.

Attributliste als Array der Größe 0 bis unbegrenzt. Wenn dieses Array leer ist, erfolgt (hierüber) keine Auswahl von Konfigurationsobjekten.

• Region[0..]

Über dieses Array können bereits definierte Regionen angegeben werden. Die Auswahl einer Region bedeutet, dass alle Konfigurationsobjekte dieser Region betrachtet werden. Wenn das Array Region leer ist, sind alle Konfigurationsobjekte ausgewählt.

• Typ[0..]

Über dieses Array werden die bisher ausgewählten Objekte auf die angegebenen Typobjekte beschränkt. D.h., wenn hier z.B. als Typ MessQuerschnitt angegeben wird, werden nur noch Konfigurationsobjekte betrachtet, die von diesem Typ stammen. Wenn hier keine Angabe erfolgt, bleibt die Auswahl bestehen.

Mengenbezeichnung

Über die Vorgabe eines Mengennamens können die Objekte ausgewählt werden, die in Mengen dieses Namens bei den ausgewählten Objekten enthalten sind. Ist hier z.B. als Menge "FahrStreifen" angegeben, wird für alle bisher ausgewählten Objekte geprüft, ob an dem Konfigurationsobjekt eine Menge dieses Namens vorhanden ist und für diesen



Fall werden die enthaltenen Konfigurationsobjekte betrachtet. Wenn hier keine Angabe erfolgt, bleibt die Auswahl bestehen.

• Objekte[0..]

Auswahl von Objekten über die explizite Angabe von einzelnen Objekten.

Attributliste als Array der Größe 0 bis unbegrenzt. Wenn dieses Array leer ist, erfolgt (hierüber) keine Auswahl von Konfigurationsobjekten.

• Objekt[0..]

Über dieses Array können beliebige Konfigurationsobjekte angegeben werden. Bei einem leeren Array sind alle Konfigurationsobjekte ausgewählt.

• Mengenbezeichnung

Über die Vorgabe eines Mengennamens können die Objekte ausgewählt werden, die in Mengen dieses Namens bei den ausgewählten Objekten enthalten sind. Ist hier z.B. als Menge "FahrStreifen" angegeben, wird für alle bisher ausgewählten Objekte geprüft, ob an dem Konfigurationsobjekt eine Menge dieses Namens vorhanden ist. Für diesen Fall werden die enthaltenen Konfigurationsobjekte betrachtet. Wenn hier keine Angabe erfolgt, bleibt die Auswahl bestehen.

2.2.2.2 AusgeschlosseneObjekte[0..]

Über diese Vorgaben werden die für die Region explizit auszuschließenden Objekte spezifiziert. Die Vorgabe kann ebenfalls über Bereiche, Regionen und einzelne Objekte parametriert werden (Kapitel 2.2.2.1 "EnthalteneObjekte[0..]").

2.2.2.3 Überlagerung der Regionen

Über die beiden Attributlisten EnthalteneObjekte und AusgeschlosseneObjekte kann detailliert definiert werden, welche Konfigurationsobjekte zu einer Region gehören. Hierbei gilt folgende Prioritätenfolge:

- Keine Aussage zu einem Konfigurationsobjekt bedeutet, dass es nicht zu der Region gehört.
- Konfigurationsobjekte, die in der Attributliste EnthalteneObjekte aufgeführt sind, gehören zu dieser Region.
- Ein Eintrag in der Attributliste AusgeschlosseneObjekte hat die höchste Priorität. Hiermit können bereits eingetragene Konfigurationsobjekte wieder eliminiert werden.

Abbildung 2-7 skizziert die Überlagerung der enthaltenen und ausgeschlossenen Objekte. Sobald durch irgendeinen Eintrag in der Attributliste ein Objekt zu den enthaltenen Objekten gehört, ist dieses Objekt im Teilergebnis enthalten. Das gleiche gilt für alle ausgeschlossenen Objekte. Beim Gesamtergebnis setzen sich die als explizit ausgeschlossenen Objekte durch.





Abbildung 2-7: Überlagerung Region

2.2.3 Parametrierung der Berechtigungsklassen

Die Berechtigungsklassen werden durch den Parameter RollenRegionenPaareParameter, der mehrere Rollen und Regionen miteinander verknüpfen kann, spezifiziert.

2.2.3.1 Rolle / Regionen - Paar

Ein Rolle / Regionen - Paar verknüpft eine Rolle (Attributgruppe Aktivitäten) und eine Region (Attributgruppe Region).

Abbildung 2-8 skizziert die Überlagerung. Auf der Abszisse sind die (atomaren) Aktivitäten der Rolle und auf der Ordinate sind die enthaltenen Objekte der Region aufgeführt, für die die entsprechenden Aktivitäten erlaubt bzw. verboten sind. Die Schnittpunkte geben jeweils an, ob die Aktivität für das entsprechende Objekt erlaubt ist oder nicht. So ist die Aktivität A 1 für das Objekt MQ 1 erlaubt und die Aktivität A 2 für das Objekt MQ 1 verboten.



Abbildung 2-8: Rolle / Regionen Paar

Version: 2.0 Status: akzeptiert





Bei der Darstellung wurden die erlaubten Kombinationen als grüne Fläche und die verbotenen Kombinationen als rote Fläche stilisiert.

Abbildung 2-9 zeigt bei dieser Darstellungsweise zwei verschieden Rollen / Regionen - Paare. Die Kombination aus der Rolle "Administrator", die alle möglichen Aktivitäten erlaubt, und der Region "Gesamt", die alle Objekte der Konfiguration enthält, wird in der Abbildung als komplett grüne Fläche dargestellt. Die Rolle "Beobachter" erlaubt als Aktivität nur, dass Datensätze zu bestimmten Attributgruppen / Aspekt - Kombinationen als Empfänger angemeldet werden dürfen. Die Kombination Rolle "Beobachter" / Region "Gesamt" ist dementsprechend gestreift dargestellt. Die Aktivitäten der grünen Streifen sind erlaubt.



Abbildung 2-9: Beispiele Rolle / Regionen Paare



2.2.3.2 Überlagerung Rolle / Regionen - Paare

Die Attributgruppe RollenRegionenPaareParameter lässt die Angabe mehrerer Rolle / Regionen - Paare zu.

Die Überlagerung zu einer Berechtigungsklasse ergibt sich durch Addition der möglichen Zugriffsrechte (s. Abbildung 2-10).



Abbildung 2-10: Überlagerung von Rolle / Regionen Paaren



2.3 Festlegung der Benutzerrechte

Einem Benutzer können eine oder mehrere Berechtigungsklassen zugewiesen werden. Bei der Vergabe mehrerer Berechtigungsklassen werden diese additiv überlagert. In diesem Fall erhält der Benutzer alle einzeln oder gemeinsam erlaubten Zugriffsrechte.

Das Beispiel in Abbildung 2-11 zeigt die Überlagerung zweier Berechtigungsklassen.

Berechtigungsklasse 1 enthält eine Gruppe von Aktivitäten, die für beliebige Objekte der Konfiguration durchgeführt werden können (Aktivitätengruppe AG₁). Die Aktivitäten der Gruppe AG₂ bis AG_i dürfen nur für Objekte der UZ Aachen durchgeführt werden. Alle anderen Kombinationen sind nicht erlaubt. Berechtigungsklasse 2 ist ähnlich aufgebaut. Hier sind erweiterte Zugriffsrechte für Objekte der UZ Köln erlaubt.

Die resultierenden Zugriffsrechte, die einem Benutzer zugeteilt sind, dem beide Berechtigungsklassen zugewiesen wurden, ist in der folgenden Abbildung skizziert.



Abbildung 2-11: Überlagerung Berechtigungsklassen



3 Einstellung der Zugriffsrechte für ein fiktives Teilsystem

In diesem Kapitel sollen die Zugriffsrechte beispielhaft für eine fiktive UZ eingestellt und aktiviert werden.

Das Teilsystem besteht aus dem Datenverteiler, der Konfiguration, der Parametrierung, der Betriebsmeldungsverwaltung, der KExTLS-Applikation, der Datenaufbereitung und -übernahme, dem Archiv und weiteren Applikationen App_j. An die UZ sollen abgesetzte Bedienungen angeschlossen werden.



Abbildung 3-1: Beispiel Unterzentrale

In Abbildung 3-1 sind die Benutzer, die für das System versorgt sein müssen, skizziert. Jede Applikation muss unter einem Benutzer gestartet werden, mit dem sich die Applikation gegenüber dem Datenverteiler authentifiziert. Die einzelnen Bediener, die über die Bedienung und Visualisierung oder den GTM die UZ bedienen wollen, müssen jeweils durch eigene Benutzerobjekte modelliert werden.



3.1 Grundsätzliche Fragestellungen

Zur Einrichtung der Zugriffsrechte müssen vorab grundsätzliche Fragestellungen geklärt werden:

- Welche Benutzer brauchen einen Zugang zu dem System?
- Wie unterscheiden sich die einzelnen Benutzer bezüglich ihrer Berechtigungen?
- Welche Berechtigungsklassen sind erforderlich?
 - Berechtigungsklassen setzen sich aus Rollen und Regionen zusammen.
 - Welche Rollen lassen sich aufgrund der unterschiedlichen Benutzerprofile definieren?
 - Welche Regionen sind sinnvoll?

Diese Fragestellungen müssen für jede autarke Organisationseinheit AOE individuell festgelegt werden.

Auf Basis der ermittelten Antworten müssen in der Konfiguration der AOE die erforderlichen Konfigurationsobjekte erstellt und verwaltet werden.



Abbildung 3-2: Erforderliche Objekte für die Zugriffsrechte

Die Parametrierung der AOE ist für die Parametrierung der zugehörigen Parameter verantwortlich.

In dem Beispiel werden die folgenden Rollen definiert:

Beobachter

Für Gäste mit sehr beschränkten Rechten (z.B. nur das Lesen bestimmter Attributgruppen/Aspekt-Kombinationen).

• Operator

Für Operatoren, Rechte für die notwendigen Aktivitäten von Operatoren. Hierzu kann z.B. das Schalten von Anzeigen oder das Quittieren oder Erstellen von Meldungen gehören.

• Verkehrstechniker

Operatorrechte mit Erweiterung z.B. Parametrierungen.



• Standardapplikation

Rechte, die eine Standardapplikation hat. Alle Applikationen müssen sich beim Start gegenüber dem Datenverteiler authentifizieren. Dazu wird eine entsprechende Berechtigungsklasse und Rolle benötigt.

• Systemmanager

z.B. zusätzliche Rechte zur Verwaltung der Zugriffsrechte.

Administrator

z.B. alle Rechte (für alle Attributgruppen / Aspekt - Kombinationen ist alles erlaubt).

Als Region wird hier nur die Region "Gesamt" vorgesehen, die alle Objekte der Konfiguration beinhaltet.

Als Berechtigungsklassen ergeben sich die Kombinationen aus den Rollen mit der Region "Gesamt".

Je Berechtigungsklasse wird jeweils ein Benutzer eingerichtet, der die entsprechenden Zugriffsrechte erhält. Damit ist es möglich, die gleichnamigen Berechtigungsklassen zu testen.

3.2 Beispiel UZ Schwelm

Jedes Teilsystem bzw. jede autarke Organisationseinheit hat ihre eigene Zugriffsrechteverwaltung. Das bedeutet, dass bei jedem System eigene Konfigurationsobjekte zur Verwaltung der Zugriffsrechte zur Verfügung stehen müssen, wenn das System über die Zugriffsrechte geschützt werden soll und eine Anbindung an weitere Systeme geplant ist. Die Konfiguration und Parametrierung der jeweiligen autarken Organisationseinheit sind jeweils für ihre Zugriffsrechte verantwortlich.

Es soll eine fiktive UZ Schwelm eingerichtet werden. Ohne Beschränkung der Allgemeinheit gehen wir nun von einem System aus, das aus den folgenden Applikationen besteht:

- Datenverteiler
- Konfiguration
- Parametrierung
- Betriebsmeldungsverwaltung

Damit die Zugriffsrechte eingestellt und aktiviert werden können, müssen die entsprechenden Objekte versorgt werden.

3.2.1 Versorgung für die Zugriffsrechte relevanten Konfigurationsobjekte

Für die UZ Schwelm wurden die folgenden Konfigurationsobjekte versorgt:

Konfigurationsobjekt	Anmerkung
Beobachter (uz.schwelm.benutzer.beobachter)	Benutzer Beobachter
Operator (uz.schwelm.benutzer.operator)	Benutzer Operator
Verkehrstechniker (uz.schwelm.benutzer. verkehrstechniker)	Benutzer Verkehrstechniker
Standardapplikation	Benutzer Standardapplikation

Zugriffsrechte Datenverteiler

Einstellung der Zugriffsrechte für ein fiktives Teilsystem



Konfigurationsobjekt	Anmerkung
(uz.schwelm.benutzer. standardapplikation)	
Systemmanager (uz.schwelm.benutzer.systemmanager)	Benutzer Systemmanager
Administrator (uz.schwelm.benutzer.administrator)	Benutzer Administrator
Beobachter (uz.schwelm.berechtigungsklasse. beobachter)	Berechtigungsklasse für Benutzer mit den ent- sprechenden Berechtigungen.
Operatoren (uz.schwelm.berechtigungsklasse. operatoren)	Berechtigungsklasse für Benutzer mit den ent- sprechenden Berechtigungen.
Verkehrstechniker (uz.schwelm.berechtigungsklasse. verkehrstechniker)	Berechtigungsklasse für Benutzer mit den ent- sprechenden Berechtigungen.
Standardapplikationen (uz.schwelm.berechtigungsklasse. standardapplikationen)	Berechtigungsklasse für Benutzer mit den ent- sprechenden Berechtigungen.
Systemmanager (uz.schwelm.berechtigungsklasse. systemmanager)	Berechtigungsklasse für Benutzer mit den ent- sprechenden Berechtigungen.
Administratoren (uz.schwelm.berechtigungsklasse. administratoren)	Berechtigungsklasse für Benutzer mit den ent- sprechenden Berechtigungen.
Beobachter (uz.schwelm.rolle.beobachter)	(Standard)Zugriffsrolle für die gleichnamige Berechtigungsklasse.
Operatoren (uz.schwelm.rolle.operatoren)	(Standard)Zugriffsrolle für die gleichnamige Berechtigungsklasse.
Verkehrstechniker (uz.schwelm.rolle. verkerhstechniker)	(Standard)Zugriffsrolle für die gleichnamige Berechtigungsklasse.
Standardapplikationen (uz.schwelm.rolle. standardapplikationen)	(Standard)Zugriffsrolle für die gleichnamige Berechtigungsklasse.
Systemmanager (uz.schwelm.rolle.Systemmanager)	(Standard)Zugriffsrolle für die gleichnamige Berechtigungsklasse.
Administratoren (uz.schwelm.rolle.administratoren)	(Standard)Zugriffsrolle für die gleichnamige Berechtigungsklasse.
Gesamt (uz.schwelm.region.gesamt)	Region, die alle Konfigurationsobjekte beinhal- tet.
Westermann (uz.schwelm.benutzer.westermann)	Benutzer Westermann Zusätzlicher Benutzer



Die erstellte Versorgungsdatei wurde in die Konfiguration der UZ Schwelm importiert und aktiviert.

An dieser Stelle soll ausdrücklich darauf hin gewiesen werden, dass die hier gewählten Benutzer, Berechtigungsklassen, Rollen und Regionen Beispiele sind. Bei jedem System müssen die grundsätzlichen Fragestellungen aus Kapitel 3.1 beantwortet werden. Aus der Analyse der sich daraus ergebenden Anforderungen werden sich dann die geeigneten Berechtigungsklassen und anderen Objekte ergeben.

3.2.2 Kurzbeschreibung der Aufrufparameter (Kernsoftware)

Im Folgenden wird an einem Beispiel gezeigt, wie ein System basierend auf der Kernsoftware eingestellt werden kann, damit die Zugriffsrechte aktiviert werden (Details siehe [BetrInf_KS]).

Datenverteiler

Als erstes wird der Datenverteiler gestartet (die angegebenen Werte sind als Beispiel zu verstehen):

```
$java \
    -cp $distributionspakete/de.bsvrz.dav.dav/de.bsvrz.dav.dav-runtime.jar \
    -Xmx200m \
    de.bsvrz.dav.dav.main.Transmitter \
    -davAppPort=8083 -davDavPort=8082 -debugFilePath=.. \
    -rechtePruefung=nein \
    -warteAufParametrierung=nein \
    -datenverteilerId=1488439676845949071 \
    -benutzer=Standardapplikation \
    -konfigurationsBenutzer=configuration \
    -parametrierung=Dasswd \
    -debugLevelStdErrText=INFO \
    -debugLevelFileText=CONFIG \
    &
```

Wichtige Aufrufparameter sind hier:

-warteAufParametrierung=ja|nein

Hiermit wird festgelegt, ob der Datenverteiler auf die Fertigmeldung der Parametrierung wartet, bevor er weitere Applikationen zulässt. Beim Aufsetzen eines Systems kann es sinnvoll sein diesen Wert auf "nein" zu setzen, da die Parametrierung noch nicht parametriert wurde und in diesem Fall (unglücklicherweise) keine Fertigmeldung absetzt, was dazu führt, dass es nicht möglich ist, z.B. mit dem GTM die Parametrierung zu parametrieren. Wenn die Parametrierung parametriert wurde, kann der Parameter gelöscht oder auf "ja" gesetzt werden.

• -rechtePruefung=nein

Hiermit wird die Rechteprüfung unterbunden. Im ersten Schritt soll mit dem GTM geprüft werden, ob die Zugriffsrechte richtig parametriert wurden. Dazu wird die Rechteprüfung ausgeschaltet.

• -datenverteilerId=zahl Hiermit wird die DatenverteilerId angegeben. Damit wird festgelegt, welches Konfigurationsobjekt den Datenverteiler repräsentiert.



-authentifizierung=passwd

Hiermit wird die Authentifizierungsdatei angegeben, in der die Login-Tolken stehen, mit denen sich die Parametrierung und die Konfiguration beim Datenverteiler authentifizieren müssen.

configuration=SRP6~~~~ 23c33c3392177514bal13c5105c894e3640c80e9bcce82dbxxxxxxxxx parameter=SRP6~~~~ 670ce5faa22ecc290046d648f8c00e89df664230565907cb5cb5xxxxxxxx AutostartApplikation=SRP6~~~~ 349d47fb8b286836e7e85998d6ecbc1864d2b1956xxxxxxxxx Standardapplikation=SRP6~~~~ 861008a6a98f7d3d2126f0690b7a97823906a41919xxxxxxxx

Abbildung 3-1: Datei passwd

- -parametrierungsBenutzer=parameter
 Hiermit wird festgelegt, dass sich die Parametrierung unter dem Benutzer parameter beim Datenverteiler anmelden muss. Der Login-Tolken, unter dem sich die Parametrierung anmelden muss, muss in der unter dem Parameter -authentifizierung zugeordneten Datei aufgeführt sein (Datei passwd).
- -konfigurationsBenutzer= configuration

Hiermit wird festgelegt, dass sich die Konfiguration unter dem Benutzer configuration beim Datenverteiler anmelden muss. Der Login-Tolken, unter dem sich die Parametrierung anmelden muss, muss in der unter dem Parameter -authentifizierung zugeordneten Datei aufgeführt sein (Datei passwd).

Konfiguration

Danach wird die Konfiguration gestartet:

```
# Konfiguration im Hintergrund starten
$java \
-cp $distributionspakete/de.bsvrz.puk.config/de.bsvrz.puk.config-runtime.jar \
-Xmx300m \
de.bsvrz.puk.config.main.ConfigurationApp \
${dav10hneAuthentifizierung} \
-benutzer=configuration \
-authentifizierung=passwd \
-verwaltung=../konfiguration/verwaltungsdaten.xml \
-benutzerverwaltung=../konfiguration/benutzerverwaltung.xml \
-debugLevelStdErrText=INF0 \
-debugLevelFileText=CONFIG \
&
```

Wichtige Aufrufparameter sind hier:

• -benutzer=configuration

Hiermit wird festgelegt, dass sich die Konfiguration unter dem Benutzer Konfiguration beim Datenverteiler anmeldet. Der Login-Tolken, unter dem sich die Parametrierung anmelden muss, muss in der unter dem Parameter -authentifizierung zugeordneten Datei aufgeführt sein (Datei passwd).

Die Authentifizierung aller Applikationen wird vom Datenverteiler mit Unterstützung der Konfiguration geprüft. Dabei ist es erforderlich, dass der entsprechenden Benutzer konfiguriert ist (dynamisches Objekt) und dass das entsprechende Login-Tolken in der Datei benutzerverwaltung.xml aufgeführt ist.

Straßen.NRW	
Tutorial	Systemberatung
Zugriffsrechte Datenverteiler	integrativ und unabhängig
Einstellung der Zugriffsrechte für ein fiktives Teilsystem	Kompetenz in System- und Verkehrstechnik
<pre><?xml version="1.0" encoding="ISO-8859-1" standalone="no"?> <!DOCTYPE benutzerkonten PUBLIC "-//K2S//DTD Authentifizierung//DE" "authentication.dt > <benutzerkonten> <benutzeridentifikation admin="ja" ja"="" name="TestDatenverteilerBenutzer" passwort="SRP6</th><th>d"> a4ab41d5555419f28c83d165eb857 6~~~ v:14ee970e03f7f5a9c885d ~ v:ae81e3a2909548daaf09baa67 89a23d408ec8859cc7e223e57023d 7f302074d8e711bcd3072d9df0ad6 4a7755274e6f3e3a6f53fcda313bb :dd5837a984c05417f9aec87d2e10 36b6467df09ff48e0a8a1f66e0d6e :0e7ae00414dbc0f1ddf1c75d44e1 ef9523cd0b2cf74e23bc9c2c2b997</benutzeridentifikation></benutzerkonten></pre>	

</benutzerkonten>



Zu einem Benutzerkonto gehören ein Benutzername, der Login-Tolken und die Rechte des Benutzers. Ein neuer Benutzer kann nur durch einen Benutzer angelegt werden, der die Rechte eines Administrators besitzt. Außerdem darf nur ein Benutzer mit Administratorrechten die Rechte eines anderen Benutzers ändern und Einmal-Passworte erzeugen. Diese Rechte werden durch das Attribut admin="ja/nein" festgelegt (Details siehe [BetrInf KS]).

Parametrierung

Danach wird die Parametrierung gestartet. An dieser Stelle wird die Parametrierung vom Basissystem VRZ (BSVRZ) verwendet.

```
$java ∖
-cp $distributionspakete/de.bsvrz.puk.param/de.bsvrz.puk.param-runtime.jar \
-Dfile.encoding=ISO-8859-1 \
de.bsvrz.puk.param.param.ParamApp \
${dav10hneAuthentifizierung} \
-benutzer=parameter \
-authentifizierung=passwd \
-persistenz=../parameter \
-persistenzModul=de.bsvrz.puk.param.param.DerbyPersistenz \
-debugLevelStdErrText=WARNING \
-debugLevelFileText=CONFIG \
&
```

Wichtige Aufrufparameter sind hier:

-benutzer= parameter

Hiermit wird festgelegt, dass sich die Parametrierung unter dem Benutzer parameter beim Datenverteiler anmeldet. Der Login-Tolken Passwort, unter dem sich die Parametrierung anmeldet, muss in der unter dem Parameter -authentifizierung zugeordneten Datei aufgeführt sein (Datei passwd).

Über den Parameter -oldDefault wird erreicht, dass die Defaultparameter zu den dynamischen Objekten (z.B. Benutzer) umgesetzt werden (Details siehe [BetrInf Param]).



Betriebsmeldungsverwaltung

Als letztes wird die Betriebsmeldungsverwaltung gestartet (im Beispiel die vereinfachte Variante SimpleMessageManager).

```
$java \
-cp $distributionspakete/de.kappich.vew.bmvew/de.kappich.vew.bmvew-runtime.jar \
de.kappich.vew.bmvew.main.SimpleMessageManager \
-datenverteiler=localhost:8083 \
-benutzer=Standardapplikation \
-authentifizierung=passwd \
-debugFilePath=.. \
-debugLevelStdErrText=WARNING \
-debugLevelFileText=CONFIG \
&
```

Wichtige Aufrufparameter sind hier:

 -benutzer=Standardapplikation
 Hiermit wird festgelegt, dass sich die Applikation unter dem Benutzer Standardapplikation beim Datenverteiler anmeldet. Das Login-Tolken, unter dem sich die Applikation anmeldet, muss in der unter dem Parameter -authentifizierung zugeordneten Datei aufgeführt sein (Datei passwd).

3.2.3 Kontrolle der Parametrierung (Erststart)

Damit die Zugriffsrechte vom Datenverteiler geprüft werden können, muss sichergestellt sein, dass die Parametrierung des Systems für die entsprechenden Parameterdaten zuständig ist. Beim Aufsetzen (ersten Start) des Systems kann es sein, dass die Parametrierung noch nicht parametriert wurde. In diesem Fall muss dies z.B. mit Hilfe des GTM durchgeführt werden. Dazu wird für die AOE der UZ Schwelm als Attributgruppe "Parametrierung" ausgewählt und der Schalter "Parameter editieren" ausgewählt. Wenn hier noch kein (Parameter)Datensatz vorhanden ist wird über den Schalter "Datensatz erzeugen" der Parameter angelegt.

. 🕘 🔍		ParameterEditor			
Auswahl					
Objekt: AOE UZ Schwelm					
Attributoruppe: Parametrie	runa	Auswahl är	ndern		
• • •					
ne Daten					
				-	
aktueller Datensatz	Datensatz erzeugen	Datensatz loschen	Kopieren	Einfugen	Senden

Abbildung 3-3: Parametrierung der Parametrierung (Erster Start)

Welche (Parameter)Attributgruppen für welche Konfigurationsobjekte durch die Parametrierung verwaltet werden müssen ist dem Datenkatalog zu entnehmen. Abbildung 2-1 skizziert das entsprechende Datenmodell.

Die Parametrierung muss für Konfigurationsobjekte der Typen Benutzer, BerechtigungsklasseNeu, RolleNeu und RegionNeu die erforderlichen Parameter Berechtigungsklassen, RollenRegionenPaare, Aktivitäten und Region vorhalten.



Im Tutorial wurde die Parametrierung so eingestellt, dass sie für alle Parameter verantwortlich ist, die an Objekten hängen, für die das System UZ Schwelm als Konfigurationsverantwortlicher zuständig ist. Diese Konfigurationsobjekte sind in der Konfigurationsbereichen versorgt, für die der Konfigurationsverantwortlicher kv.uz.schwelm als Konfigurationsverantwortlicher eingetragen ist.

usuvali bytek: AC UZ Schweim ttributgruppe: Parametrierung g.parametrierung: Urlasser: BenutzerReferenz: undefiniert Ursache: Vranlasser: ParameterSatz: Arraygröße: 1 0 0 0: Bereich: Arraygröße: S 0 0 0 1: kb.uz.schweim pid (Name: Defaultbereich der UZ Schweim) 0 0: kb.default.uz.schweim pid (Name: Systemobjekte der UZ Schweim) 0 1: kb.uz.schweim pid (Name: Systemobjekte der UZ Schweim) 0 1: kb.uz.schweim pid (Name: Systemobjekte der UZ Schweim) 0 1: kb.uz.griffsrechte.uz.schweim pid (Name: Zugriffsrechte der UZ Schweim) 0 1: kb.uz.griffsrechte.uz.schweim pid (Name: Zugriffsrechte der UZ Schweim) 0 0: DatenSpezifikation: Arraygröße: 0 0 0: Einstellungen: 0: 0: Parametrieren 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:	• •	ParameterEditor
atueller Datensatz Datensatz Datensatz Datensatz Datensatz Datensatz Socie Socie <th>uswahl bjekt: AOE UZ Schwelm</th> <th>Auswahl ändern</th>	uswahl bjekt: AOE UZ Schwelm	Auswahl ändern
g, parametrierung: Urlasser: BenutzerReferenz: undefiniert Ursache: Veranlasser: ParameterSatz: Arraygröße: 1 0 0 Bereich: Arraygröße: 5 0 0 0 0 0: Bereich: Arraygröße: 5 0 0 0 1 0: kb.default.uz.schwelm pid (Name: Defaultbereich der UZ Schwelm) 0 2 0: kb.default.uz.schwelm pid (Name: Konfigurationsverantwortlicher (AOE) der UZ Schwelm) 0 2 0: kb.system.uz.schwelm pid (Name: Systemobjekte der UZ Schwelm) 0 3 0: kb.objekte.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 0 0 0: 0 0:	.ttributgruppe: Parametrierung	
Urlasser: BenutzerReferenz: undefiniert Ursache: Veranlasser: ParametrSatz: Arraygröße: 1 0 0 Bereich: Arraygröße: 5 0 0 0 1 kb.default.uz.schwelm pid (Name: Defaultbereich der UZ Schwelm) 0 2 kb.vstem.uz.schwelm pid (Name: Konfigurationsverantwortlicher (AOE) der UZ Schwelm) 0 2 kb.system.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 0 3 kb.objekte.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 0 4 kb.zugriffsrechte.uz.schwelm pid (Name: Zugriffsrechte der UZ Schwelm) 0 0 bjekt: Arraygröße: 0 0 0 1 cm 5 simulationsVariante: 0 5 simulationsVariante: 0 5 simulationsVariante: 0 5 million 0	g.parametrierung:	
BenutzerReferenz: undefiniert Ursache: Veranlasser: ParametrSatz: Arraygröße: 1 • • • • • • • • • • • • • • • • • • •	Urlasser:	
Ursache: Veranlasser: ParameterSatz: Arraygröße: 1 0 0 0: kb.default.uz.schwelm pid (Name: Defaultbereich der UZ Schwelm) 0 0 1: kb.uz.schwelm pid (Name: Konfigurationsverantwortlicher (AOE) der UZ Schwelm) 0 0 2: kb.system.uz.schwelm pid (Name: Systemobjekte der UZ Schwelm) 0 0 0 0 3: kb.objekte.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 0 0 0 0 0: Objekt: Arraygröße: 1 0 0 0: Objekt: Arraygröße: 0 0 0 0: Objekt: 0: Objekt:	BenutzerReferenz: undefiniert	
Veraniasser: ParameterSatz: Arraygröße: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Ursache:	
Arraygröße: 1 0 0 Ø: Bereich: Arraygröße: S 0 0 0 1: kb.default.uz.schwelm pid (Name: Defaultbereich der UZ Schwelm) 0 0 0 2: kb.system.uz.schwelm pid (Name: Konfigurationsverantwortlicher (AOE) der UZ Schwelm) 0 0 0 3: kb.objekte.uz.schwelm pid (Name: Systemobjekte der UZ Schwelm) 3: kb.objekte.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 4: kb.zugriffsrechte.uz.schwelm pid (Name: Zugriffsrechte der UZ Schwelm) DatenSpezifikation: Arraygröße: 0 0 0 0 Arraygröße: 0 0 0 0 0 0 AttributGruppe: Arraygröße: 0 0 0 Arraygröße: 0 0 0 0 SimulationsVariante: 0 0 Ø Parametrieren 0 0 Ø Parametrieren 0 0	veraniasser:	
Arraygröße: 1 Image: State of the s	ParameterSatz:	
Bereich: Arraygröße: 5 ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° °	Arraygroise: 1 C P	
Arraygröße: 5) > 0: kb.default.uz.schwelm pid (Name: Defaultbereich der UZ Schwelm) > > 1: kb.uz.schwelm pid (Name: Systemobjekte der UZ Schwelm) > > > 2: kb.system.uz.schwelm pid (Name: Systemobjekte der UZ Schwelm) > >	G.	
0: kb.default.uz.schwelm pid (Name: Defaultbereich der UZ Schwelm) 1: kb.uz.schwelm pid (Name: Systemobjekte der UZ Schwelm) 2: kb.system.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 3: kb.objekte.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 4: kb.zugriffsrechte.uz.schwelm pid (Name: Zugriffsrechte der UZ Schwelm) 5: mid (Name: Systemobjekte der UZ Schwelm) mid (Name: Systemobjekte der UZ Schwelm) 6: mid (Name: Zugriffsrechte der UZ Schwelm) mid (Name: Systemobjekte der UZ Schwelm) 6: mid (Name: Zugriffsrechte der UZ Schwelm) mid (Name: Systemobjekte der UZ Schwelm) 6: mid (Name: Zugriffsrechte der UZ Schwelm) mid (Name: Systemobjekte der UZ Schwelm) 6: mid (Name: Zugriffsrechte der UZ Schwelm) mid (Name: Systemobjekte der UZ Schwelm) 6: mid (Name: Zugriffsrechte der UZ Schwelm) mid (Name: Zugriffsrechte der UZ Schwelm) 0: mid (Name: Zugriffsrechte der UZ Schwelm) mid (Name: Zugriffsrechte der UZ Schwelm) 0: mid (Name: Zugriffsrechte der UZ Schwelm) mid (Name: Zugriffsrechte der UZ Schwelm) 0: mid (Name: Zugriffsrechte der UZ Schwelm) mid (Name: Zugriffsrechte der UZ Schwelm) 0:	Arraygröße: 5 🗘 🖶 📷	
1: kb.uz.schwelm pid (Name: Konfigurationsverantwortlicher (AOE) der UZ Schwelm) 2: kb.system.uz.schwelm pid (Name: Systemobjekte der UZ Schwelm) 3: kb.objekte.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 4: kb.zugriffsrechte.uz.schwelm pid (Name: Zugriffsrechte der UZ Schwelm) 4: kb.zugriffsrechte.uz.schwelm pid (Name: Zugriffsrechte der UZ Schwelm) 6: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: SimulationsVariante: 0: 0: image: 0: 0: 0: 0: image: 0: 0: 0: 0: image: </th <th>0: kb.default.uz.schwelm</th> <th>pid (Name: Defaultbereich der UZ Schwelm) 🕋 💮 🛅 🥅</th>	0: kb.default.uz.schwelm	pid (Name: Defaultbereich der UZ Schwelm) 🕋 💮 🛅 🥅
2: kb.system.uz.schwelm pid (Name: Systemobjekte der UZ Schwelm) 3: kb.objekte.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 4: kb.zugriffsrechte.uz.schwelm pid (Name: Zugriffsrechte der UZ Schwelm) DatenSpezifikation: Arraygröße: 1 0 0: 0 0 0 Objekt: Arraygröße: 0 0 0 AttributGruppe: Arraygröße: 0 0 0 SimulationsVariante: 0 0 0 Einstellungen: 0 0 0 0 Aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se	1: kb.uz.schwelm pid (Name: Konfigura	rationsverantwortlicher (AOE) der UZ Schwelm) 📄 🚭 🗟 🗈 😑
3: kb.objekte.uz.schwelm pid (Name: Verkehrsobjekte der UZ Schwelm) 4: kb.zugriffsrechte.uz.schwelm pid (Name: Zugriffsrechte der UZ Schwelm) DatenSpezifikation: Arraygröße: 1 Arraygröße: 1 1 0: Objekt: Arraygröße: 0 Arraygröße: 0 1 1 Arraygröße: 0 1 1 SimulationsVariante: 0 1 1 Einstellungen: 1 1 1 Ø Parametrieren 1 1 aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se	2: kb.system.uz.schwelm	pid (Name: Systemobjekte der UZ Schwelm) 🗎 🖶 🗟 🗓 😑
4: kb.zugriffsrechte.uz.schwelm pid (Name: Zugriffsrechte der UZ Schwelm) Pie	3: kb.objekte.uz.schwelm	pid (Name: Verkehrsobjekte der UZ Schwelm) 📄 💮 🗟 🗊 😑
DatenSpezifikation: Arraygröße: 1 0: Objekt: Arraygröße: 0 AttributGruppe: Arraygröße: 0 SimulationsVariante: 0 Einstellungen: Ø Parametrieren aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren	4: kb.zugriffsrechte.uz.schwelm	pid (Name: Zugriffsrechte der UZ Schwelm) 📄 🚭 🗟 📳 😑
Arraygröße: 1 C C O: Objekt: Arraygröße: 0 C C C AttributGruppe: Arraygröße: AttributGruppe: Arraygröße: AttributGruppe: C C C Arraygröße: 0 C C C SimulationsVariante: 0 C C C C Parametrieren C C C aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se	DatenSpezifikation:	
O: Objekt: Arraygröße: O C P P AttributGruppe: AttributGruppe: Arraygröße: O C P P SimulationsVariante: O Einstellungen: Parametrieren Ø Parametrieren P P aktueller Datensatz Datensatz erzeugen Datensatz löschen	Arraygröße: 1 🗘 😭	
Arraygröße: 0 C C C C AttributGruppe: Arraygröße: 0 C C C C C SimulationsVariante: 0 C C C C C C C C C C C C C C C C C C C	0:	
AttributGruppe: Arraygröße: 0 SimulationsVariante: 0 Einstellungen: Image: I	Arraygröße: 0 🗘 🖶 📷	
Arraygröße: 0 Image: Constrainte: Image: Cons	AttributGruppe:	
SimulationsVariante: 0	Arraygröße: 0 🗘 🖶 📷	
Einstellungen: Parametrieren Aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se	SimulationsVariante: 0	•
Einstellungen: Parametrieren aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se		
✓ Parametrieren ▲ I □ ▲ I □ aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se	Einstellungen:	
aktueller Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se	Parametrieren	
aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se		
aktueller Datensatz Datensatz erzeugen Datensatz löschen Kopieren Einfügen Se		
aktuener Datensatz inschen Datensatz inschen Kopieren Einfugen Se	aktueller Datensatz	Datensatz löschen Konieren Finfügen S
		Successive reserver and a successive reserve

Abbildung 3-4: Parametrierung der Parametrierung

Nachdem gewährleistet ist, dass die Parametrierung die erforderlichen Daten verwaltet, werden die Parameter zu den einzelnen Benutzern, Berechtigungsklassen, Rollen und Regionen eingestellt bzw. kontrolliert.



3.2.3.1 Benutzer

Mit dem GTM werden alle Objekte vom Typ Benutzer kontrolliert.

Objekttyp	1 / 75	× ►	Objekte 1 / 9	Kannich
Benutzer (typ. benutzer) BerechtigungsklasseNet (typ. berechtigungsklasse) BerechtigungsklasseNeu (typ. berechtigungsklasseNeu) BertriebsMeldungsVerwaltung (typ. betriebsMeldungsVerwaltung) DatenAuswahl (typ. datenAuswahl) Datenverteiler (typ. datenverteiler)		0	Administrator (uz.schwelm.benutzer.administrator) Beobachter (uz.schwelm.benutzer.beobachter) Operator (uz.schwelm.benutzer.operator) Standardapplikation (uz.schwelm.benutzer.standardapplikation) Systemmanager (uz.schwelm.benutzer.systemmanager) TestDatenverteilerBenutzer (benutzer.testDatenverteiler)	Bystemberatung Integrativ und unabhängig Kompanie a bysten und visiokastenist
Attributgruppe	1/8	×	Tester (benutzer.tester) Verkehrstechniker (uz.schwelm.benutzer.verkehrstechniker)	Datenverfügbarkeitsprüfung
AlternativeObjektbezeichnung (atg.alternativeObjektbezeichnung	j)		Westermann (uz.schwelm.benutzer.westermann)	Onlinetabelle anzeigen
BenutzerEigenschaften (atg.benutzerEigenschaften) BenutzerNachricht (atg.benutzerNachricht)				Konfigurationsdaten anzeigen
BenutzerParameter (atg.benutzerParameter) Berechtigungsklassen (atg.berechtigungsklassen)				Aktuelle Daten anzeigen
INTO (atg.Into)				Aktuelle Daten senden
Aspekt	0/4	×		Archivanfrage (Stream)
Default-Parameter–Aspekt (asp.parameterDefault) Ist-Parameter–Aspekt (asp.parameterIst) Soll-Parameter–Aspekt (asp.parameterSoll)				Archiv-Information
Vorgabe-Parameter-Aspekt (asp.parameterVorgabe)				Systemprotokollierer starten
				Onlineprotokollierer starten
Simulationsvariante:	(00		Anmeldungen

Abbildung 3-5: Parametrierung der Benutzer

Die Liste der Objekte entspricht den Vorgaben der Versorgung (s. Kapitel 3.2.1 "Versorgung für die Zugriffsrechte relevanten Konfigurationsobjekte").

Dem Benutzer Westermann wird die Berechtigungsklasse Administratoren zugewiesen (Attribut Berechtigungsklassen (Array)). Anschließend werden die vergebenen Berechtigungsklassen der Benutzer kontrolliert.

		ParameterEditor				
Auswahl Objekt: Westermann	• • •	Objekte vom	Typ Berecht	tigungsklasseNeu hinzufüge	n	
Attributgruppe: Berechtigungsklassen	Objekttyp		1/2 🗙 🖡	Objekte	[1/6 🗙
atg.berechtigungsklassen: Urlasser: BenutzerReferenz: undefiniert Ursache: Veranlasser: Berechtigungsklassen: Arraygröße: 0 🗘 🖨 📷	BerechtigungsklasseNe KonfigurationsObjekt (t	u (typ.berechtigungskla yp.konfigurationsObjel	sseNeu) t)	Administratoren (uz.schwelin Beobachter (uz.schwelm.be Operatoren (uz.schwelm.be Standardapplikationen (uz. Systemmanager (uz.schwelr Verkehrstechniker (uz.schw	n. berechtigungsklasse. a rechtigungsklasse. beob rechtigungsklasse. opera chwelm. berechtigungsklasse. s elm. berechtigungsklasse. elm. berechtigungsklasse	dministre achter) itoren) lasse.stan ystemmar 2.verkehrs
					OK Abbre	chen
aktueller Datensatz Datensatz er	zeugen Datensa	itz löschen K	opieren	Einfügen Send	en	

Abbildung 3-6: Parametrierung des Benutzers Westermann (Berechtigungsklassen)



				Berechtigungsklassen	4
Art	Zeit	Objekt		Berechtigungsklassen []	•
OA	11.04.2019 19:01:44,541	Westermann	·	uz.schwelm.berechtigungsklasse.administratoren pid (Name: Administratoren)	
OA	11.04.2019 18:37:49,923	Administrator	·		
OA	11.04.2019 18:37:49,923	Beobachter	·II		
OA	11.04.2019 18:37:49,923	Operator	·II		
OA	11.04.2019 18:37:49,923	Standardapplikation	٠I		
OA	11.04.2019 18:37:49,923	Systemmanager	٠I		
OA	11.04.2019 19:01:56,940	TestDatenverteilerBenutzer	ke	eine Daten (keine Quelle)	
OA	11.04.2019 19:01:56,940	Tester	ke	ine Daten (keine Quelle)	
OA	11.04.2019 18:37:49,923	Verkehrstechniker	П		

Abbildung 3-7: Kontrolle der Benutzerparameter

In dem Beispiel wurden noch die Benutzer Administrator, Beobachter, Operator, Standardapplikation, Systemmanager und Verkehrstechniker unter dem Konfigurationsverantwortlichen kv.uz.schwelm angelegt. Dabei fällt bei der Kontrolle auf, dass diesen Benutzern noch keine Berechtigungsklasse zugewiesen wurde. Das bedeutet, dass bei eingeschalteter Rechteprüfung diesen Benutzern kein Zugriff gewährt wird.

Da die Applikationen der UZ Schwelm unter dem Benutzer Standardapplikation laufen sollen, muss zumindest diesem Benutzer eine Berechtigungsklasse zugewiesen werden, die i.d.R. alle Rechte erhält.

In dem Tutorial wurden für die einzeln Aufgaben und Befugnisse, die einzurichtende Benutzer haben sollen entsprechende Berechtigungsklassen definiert, die im Folgenden den Benutzern zugewiesen wurden.

				Berechtigungsklassen
Art	Zeit	Objekt		Berechtigungsklassen []
OA	11.04.2019 19:19:41,646	Administrator		uz.schwelm.berechtigungsklasse.administratoren pid (Name: Administratoren)
OA	11.04.2019 19:20:02,077	Beobachter		uz.schwelm.berechtigungsklasse.beobachter pid (Name: Beobachter)
OA	11.04.2019 19:20:58,102	Operator		uz.schwelm.berechtigungsklasse.operatoren pid (Name: Operatoren)
OA	11.04.2019 19:19:14,710	Standardapplikation		uz.schwelm.berechtigungsklasse.standardapplikationen pid (Name: Standardapplikationen)
OA	11.04.2019 19:20:14,909	Systemmanager		uz.schwelm.berechtigungsklasse.systemmanager pid (Name: Systemmanager)
OA	11.04.2019 19:01:56,940	TestDatenverteilerBenutzer	k	eine Daten (keine Quelle)
OA	11.04.2019 19:01:56,940	Tester	k	eine Daten (keine Quelle)
OA	11.04.2019 19:20:29,970	Verkehrstechniker		uz.schwelm.berechtigungsklasse.verkehrstechniker pid (Name: Verkehrstechniker)
OA	11.04.2019 19:01:44,541	Westermann		uz.schwelm.berechtigungsklasse.administratoren pid (Name: Administratoren)

Abbildung 3-8: Benutzerparameter nach Durchführung der Parametrierung

Die Benutzer TestDatenverteilerBenutzer und Tester werden durch das System nicht parametriert, da sie in Konfigurationsbereichen versorgt wurden, die nicht unter dem Konfigurationsverantwortlichen kv.uz.schwelm stehen.



3.2.3.2 Berechtigungsklassen

Mit dem GTM werden alle Objekte vom Typ BerechtigungsklasseNeu kontrolliert bzw. versorgt.

	110	ppien oyster	_	-	1000111031.00	000			
Objekttyp Benutzer (typ.benutzer) BerechtigungsklasseAlt (typ.berechtigungsklasse) BereibsMeldungsVerwaltung (typ.betriebsMeldungsVern DatenAuswahl (typ.datenAuswahl) Attributgruppe AlternativeObjektbezeichnung (atg.alternativeObjektbez Default-Parameterdatensätze (atg.defaultParameterdat Info (atg.info) RollenRegionenPaare (atg.rollenRegionenPaare) Default-Parameter-Aspekt (asp.parameterDefault) Ist-Parameter-Aspekt (asp.parameterSoll) Vorgabe-Parameter-Aspekt (asp.parameterSoll) Vorgabe-Parameter-Aspekt (asp.parameterVorgabe)		1 / 86 rwaltung) 1 / 4 ezeichnung) 1 / 4 1 / 4	 Objekte Objekte Objekte Administratoren (uz.schwelm.berechtigungsklasse.administratoren (uz.schwelm.berechtigungsklasse.beobachter) Operatoren (uz.schwelm.berechtigungsklasse.operatoren) Standardapplikationen (uz.schwelm.berechtigungsklasse.stan Systemmanager (uz.schwelm.berechtigungsklasse.systemmar Verkehrstechniker (uz.schwelm.berechtigungsklasse.verkehrstechniker) 				Respective and unabhinging Parameter editieren Onlinetabelle anzeigen Konfigurationsdaten anzeigen Aktuelle Daten anzeigen Aktuelle Daten senden Archivanfrage (Stream) Systemprotokollierer starte Onlineprotokollierer starte		
Ist-Parameter-Aspekt (asp Soll-Parameter-Aspekt (as Vorgabe-Parameter-Aspe	o.parameterist) sp.parameterSoll) kt (asp.parameterVorgabe)						Onlineprotokollierer starten		
Ist-Parameter-Aspekt (asg Soll-Parameter-Aspekt (as Vorgabe-Parameter-Aspe Simulationsvariante:	s.parameterist) ;p.parameterSoll) kt (asp.parameterVorgabe)	0					Onlineprotokollierer starten Datengenerator Anmeldungen		
Ist-Parameter-Aspekt (asp Soll-Parameter-Aspekt (as Vorgabe-Parameter-Aspe Simulationsvariante:	s.parameterist) ip.parameterSoll) kt (asp.parameterVorgabe)	0					Onlineprotokollierer starten Datengenerator Anmeldungen		
Ist-Parameter-Aspekt (asg Soll-Parameter-Aspekt (as Vorgabe-Parameter-Aspe Simulationsvariante:	o.parameterist) (p.parameterSoll) kt (asp.parameterVorgabe) Onlinetabelle (A	0 ttributgruppe] 🗘	lenRegionenPaare, Aspekt: Soll-Parar	meter-Aspek	t) - localhost:808:	Onlineprotokollierer starten Datengenerator Anmeldungen		
Ist-Parameter-Aspekt (asp Soll-Parameter-Aspekt (asp Vorgabe-Parameter-Aspe Simulationsvariante:	.parameterist) p.parameterSoll) kt (asp.parameterVorgabe) Onlinetabelle (A	0 ttributgruppe) 🗘	e lenRegionenPaare, Aspekt: Soll-Parar RollenR	meter-Aspek RegionenPaa	t) - localhost:808: re	Onlineprotokollierer starten Datengenerator Anmeldungen		
Ist-Parameter-Aspekt (asp Soll-Parameter-Aspekt (as Vorgabe-Parameter-Aspe Simulationsvariante: Zeit	oparameterist) p. parameterSoll) kt (asp. parameterVorgabe) Onlinetabelle (A Objekt	0 ttributgruppe] () 2: Rol	lenRegionenPaare, Aspekt: Soll-Parar RollenR RollenR	meter-Aspek RegionenPaa RegionenPaa	t) - localhost:808: re re []	Onlineprotokollierer starten Datengenerator Anmeldungen		
Ist-Parameter-Aspekt (asp Soll-Parameter-Aspekt (asp Vorgabe-Parameter-Aspe Simulationsvariante:	Onlinetabelle (A Objekt	0 ttributgruppe] 🕽	lenRegionenPaare, Aspekt: Soll-Parar RollenR Rolle	meter-Aspek RegionenPaar RegionenPaar	t) - localhost:808: re re []	Onlineprotokollierer starten Datengenerator Anmeldungen 3 Ameldungen 4 Region 4		
Ist-Parameter-Aspekt (asp Soll-Parameter-Aspekt (asp Vorgabe-Parameter-Aspekt Simulationsvariante: Zeit 29.05.2019 12:18:39.953	Onlinetabelle (A Objekt Administratoren	0 ttributgruppe	C Rol	lenRegionenPaare, Aspekt: Soll-Parar RollenR Rollen Rolle administratoren pid (Name: Administratoren)	meter-Aspek RegionenPaar KegionenPaar	t) - localhost:8083 re re [] iz.schwelm.region.ges	Onlineprotokollierer starten Datengenerator Anmeldungen		
Ist-Parameter-Aspekt (as; Soll-Parameter-Aspekt (as; Vorgabe-Parameter-Aspe Simulationsvariante: Zeit 29.05.2019 12:18:39.953 29.05.2019 12:18:40.037	Onlinetabelle (A Onlinetabelle (A Objekt Administratoren Beobachter	0 ttributgruppe 	.rolle	IenRegionenPaare, Aspekt: Soll-Parar Rollen Rollen Rolle administratoren pid (Name: Administratoren) beobachter pid (Name: Beobachter)	meter-Aspek RegionenPaar RegionenPaar ()	t) - localhost:8083 re re [] z.schwelm.region.ges z.schwelm.region.ges	Onlineprotokollierer starten Datengenerator Anmeldungen		
Ist-Parameter-Aspekt (asp Soll-Parameter-Aspekt (asp Vorgabe-Parameter-Aspekt (as Vorgabe-Parameter-Aspe Simulationsvariante: 29,05,2019 12:18:39,953 29,05,2019 12:18:39,953 29,05,2019 12:18:39,953	Onlinetabelle (A Objekt Administratoren Beobachter Operatoren	0 ttributgruppe	rolle	lenRegionenPaare, Aspekt: Soll-Parar Rollen& Rollen& administratoren pid (Name: Administratoren) beobachter pid (Name: Operatoren)	meter-Aspek RegionenPaar RegionenPaar U	t) - localhost:808 re re [] zz.schweim.region.ges zz.schweim.region.ges	Onlineprotokollierer starten Datengenerator Anmeldungen		
Ist-Parameter-Aspekt (as; Soll-Parameter-Aspekt (as; Soll-Parameter-Aspekt (as; Vorgabe-Parameter-Aspekt Simulationsvariante: Zeit 29.05.2019 12:18:39.953 29.05.2019 12:18:40.037 29.05.2019 12:18:40.037	Onlinetabelle (A Onlinetabelle (A Objekt Administratoren Beobachter Standardapplikationen	0 ttributgruppe	rolle rolle	IenRegionenPaare, Aspekt: Soll-Parar RollenR Rollen administratoren pid (Name: Administratoren) beobachter pid (Name: Beobachter) operatoren pid (Name: Operatoren) standardapplikationen pid (Name: Standardappi	meter-Aspek RegionenPaar « u u u u u u u u u u u u u u u u u	t) - localhost:808 re re [] iz.schwelm.region.ges iz.schwelm.region.ges iz.schwelm.region.ges	Onlineprotokollierer starten Datengenerator Anmeldungen Region 4 Region 4 mt pid (Name: Gesamt) amt pid (Name: Gesamt) amt pid (Name: Gesamt)		
Ist-Parameter-Aspekt (as; Soll-Parameter-Aspekt (as; Vorgabe-Parameter-Aspe Simulationsvariante: Zeit 29.05.2019 12:18:39.953 29.05.2019 12:18:40.037 29.05.2019 12:18:40.037 29.05.2019 12:18:40.037 29.05.2019 12:18:40.037	Onlinetabelle (A Onlinetabelle (A Objekt Administratoren Beobachter Standardapplikationen Standardapplikationen	0 ttributgruppe (4) >>> Uz.schwelm Uz.schwelm Uz.schwelm Uz.schwelm Uz.schwelm Uz.schwelm	rolle rolle rolle rolle	IenRegionenPaare, Aspekt: Soll-Parar Rollena Rollena Administratoren pid (Name: Administratoren) beobachter pid (Name: Sobachter) operatoren pid (Name: Sobachter) standardapplikationen pid (Name: Standardap systemmanager) pid (Name: Standardap	meter-Aspek RegionenPaa RegionenPaa U U U U U U U U U U U U U U U U U U	t) - localhost:808 re re z. schwelm.region.ges z. schwelm.region.ges z. schwelm.region.ges z. schwelm.region.ges	Onlineprotokollierer starten Datengenerator Anmeldungen		

Abbildung 3-9: Parametrierung der Berechtigungsklassen

Die aufgelisteten Objekte entsprechen der Versorgung (s. Kapitel 3.2.1 "Versorgung für die Zugriffsrechte relevanten Konfigurationsobjekte").



3.2.3.3 Rollen

Mit dem GTM werden alle Objekte vom Typ RolleNeu kontrolliert bzw. versorgt.

		0	4			
Objekttyp	1 / 86	×	►	Objekte	6/6 🗙	Kappich
RolleAlt (typ.zugriffsRolle)				Administratoren (uz.schwelm.rolle.administr	ratoren)	Systemberatung
RolleNeu (typ.zugriffsRolleNeu)				Beobachter (uz.schwelm.rolle.beobachter)		integrativ und unabhängig
SimulationsVerwaltung (typ.simulationsVerwalt	ung)			Operatoren (uz.schwelm.rolle.operatoren)		Promposition in objective and detailementer
StörfallIndikator (tvp.störfallIndikator)				Standardapplikationen (uz.schwelm.rolle.sta	andardapplikation	
				Systemmanager (uz.schweim.rolle.systemm	anager)	Parameter editieren
Attributgruppe	1/4	×		verkenrstechniker (uz.schweim.rolie.verken	rstechniker)	Onlinetabelle anzeigen
Aktivitäten (atg.rollenAktivität)						Oninetabelle anzeigen
AlternativeObjektbezeichnung (atg.alternative	Objektbezeichnung)					Konfigurationsdaten anzeigen
Default-Parameterdatensätze (atg.defaultPara	meterdatensätze)		0			
Info (atg.info)						Aktuelle Daten anzeigen
Aspekt	1/4	×				Aktuelle Daten senden
Default-Parameter-Aspekt (asp.parameterDe	fault)					Archivanfrage (Stream)
lst-Parameter-Aspekt (asp.parameterlst)						
Soll-Parameter-Aspekt (asp.parameterSoll)						
Vorgabe-Parameter-Aspekt (asp.parameterV	orgabe)					Systemprotokollierer starten
Simulationsvariante:	0	0				Onlineprotokollierer starten

Abbildung 3-10: Parametrierung der Zugriffsrollen

•	•					Online	tabelle (/	ttributg	ruppe: A	ktivitäten, Aspe	kt: Soll-Parameter-Aspekt) -	localhost:8083				
			1								Aktivität	en				4
An	Zeit	Objekt	44		Akt	ivitätDaten [.	.1		4		AktivitätObjek	te []		AktivitätMengen []	4	0-11-
			+++	Name		Empfän	Sen <	Qu4	Se 4	Objekttyp4	Konfigurationsbereich4	ObjekteErzeugenÄndernLösc <	Mengentyp4	Konfigurationsbereich	MengeÄnd <	Kolle4
0A	12.04.2019 10:58:35,993	Administratoren	H	General	Π	Ja	la	Ja	la	typ.dynamisches typ.konfiguratio		la			Ja	
OA	12.04.2019 11:08:31,003	Beobachter		GeneralEmpfänger		la	Nein	Nein	Nein							
OA	12.04.2019 11:09:19.971	Operatoren		GeneralEmpfängerSender		Ja	Ja	Nein	Nein	typ.dynamisches		Ja			Ja	
0A	12.04.2019 11:01:08,287	Standardapplikationen		General		Ja	Ja	Ja	la	typ.dynamisches typ.konfiguratio		Ja			Ja	
0A	12.04.2019 11:01:25,644	Systemmanager	P	General	Π	Ja	Ja	Ja	la	typ.dynamisches typ.konfiguratio		Ja			Ja	
0A	12.04.2019 11:01:43,782	Verkehrstechniker		General		la	Ja	Ja	Ja	typ.dynamisches typ.konfiguratio		Ja			Ja	

Abbildung 3-11: Parametrierung der Zugriffsrollen (Übersicht)

Die aufgelisteten Objekte entsprechen der Versorgung (s. Kapitel 3.2.1 "Versorgung für die Zugriffsrechte relevanten Konfigurationsobjekte).

Der Parametersatz für die Zugriffsrolle Administrator ist in Abbildung 3-12 dargestellt.

Hier sind sämtliche Aktivitäten erlaubt. Deshalb wurde als beschreibender Name "General" gewählt. Bei der Datenaktivität sind keine Einschränkungen bzgl. Konfigurationsbereich, Attributgruppe oder Aspekt vorgegeben. Damit sind die folgenden Aktionen für alle möglichen Kombinationen erlaubt (Wildcard). Über die Felder können explizit Einschränkungen vorgegeben werden. Bei der Auswahl von Attributgruppen und Aspekten werden die Aktionen auf die möglichen Kombination von Attributgruppe und Aspekt eingeschränkt. Der Administrator darf zu alle möglichen Kombinationen Daten als Empfänger; Sender, Quelle oder Senke anmelden.

Weiter darf der Administrator beliebige Objekte neu anlegen oder löschen (da alle Objekttypen entweder vom Typ Dynamisches oder Konfigurations-Objekt abgeleitet sind). Er darf beliebige Mengen ändern.

Die Zugriffsrolle Standardapplikation sollte ebenfalls umfassende Rechte haben, da mit dieser Zugriffsrolle die Applikationen des Systems gestartet werden.



Auswahl ändern g.rollenAktivität: Urlasser: BenutzerReferenz: Ursache: Defaultversorgung Veranlasser: AktivitätDaten: Arraygröße: 1 Arraygröße: 0 Name: General Konfigurationsbereich: Arraygröße: 0 Attributgruppe: Arraygröße: 0 Attributgruppe: Arraygröße: 0 Implanger: ja Sender: ja Ouelle: ja Senke: ja Objekttyp: Arraygröße: 2	
g.rollenAktivität: Urlasser: BenutzerReferenz: undefiniert Ursache: Defaultversorgung Veranlasser: AktivitätDaten: Arraygröße: 1 0 0 0: Name: General Konfigurationsbereich: Arraygröße: 0 0 0 Attributgruppe: Arraygröße: 0 0 0 Empfänger: Ja Sender: Ja Quelle: Ja Senke: Ja AktivitätObjekte: Arraygröße: 1 0 0: Objekttyp: Arraygröße: 2 0 0 Image: Sender: Ja	
Jrlasser:	
Benutzerkeferenz: undefiniert Ursache: Defaultversorgung Veranlasser:	
Ursache: Defailtversorgung Veranlasser: Atraygröße: 1 Arraygröße: 1 O: Name: Ceneral Konfigurationsbereich: Arraygröße: O: Attributgruppe: Arraygröße: O: Arraygröße: O: Arraygröße: Image: Image: <tr< td=""><td></td></tr<>	
AktivitätDaten: Arraygröße: 1 Arraygröße: 0 Name: Ceneral Konfigurationsbereich: Arraygröße: 0 Attributgruppe: Arraygröße: 0 4 Arraygröße: 0 4 Arraygröße: 0 4<	
Arraygröße: 1 1 0: Name: Ceneral Konfigurationsbereich: Arraygröße: 0 Attributgruppe: Arraygröße: 0 Ceneral Arraygröße: 0 Ceneral Arraygröße: 0 Ceneral Arraygröße: 1 Ceneral Arraygröße: 1 Ceneral O: O: Objekttyp: Arraygröße: 2 Ceneral Ceneral Ceneral Arraygröße: 2 Ceneral Ceneral <td></td>	
Name: Ceneral Konfigurationsbereich: Arraygröße: 0 Attributgruppe: Arraygröße: 0 Construction O: O: Objekttyp: Arraygröße: 2 Construction	
Konfigurationsbereich: Arraygröße: 0 Attributgruppe: Arraygröße: 0 Capacity Arraygröße: 0 Cotype: Otype: Otype: <td></td>	
Arraygröße: 0 C I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	
Attributgruppe: Arraygröße: 0 0 4 in	
Arraygröße: 0 Aspekt: Arraygröße: 0 Empfänger: Ja Sender: Ja Quelle: Ja Senke: Ja Arraygröße: 1 0: Objekttyp: Arraygröße: 2 Image: Arraygröße: 2 Image: Ima	
Aspekt: Arraygröße: 0 C C C C C C C C C C C C C C C C C C	
Arraygröße: 0 Empfänger: ja Sender: ja Quelle: ja Senke: ja Senke: ja O: I Objekttyp: I Arraygröße: 2 Image:	
Empfänger: Ja Sender: Ja Quelle: Ja Senke: Ja KtivitätObjekte: Arraygröße: 1 0 0 O: Objekttyp: Arraygröße: 2 0 0 0000000000000000000000000000000	
Sender: Ja Quelle: Ja Senke: Ja Arraygröße: 1 0 0 O: Objekttyp: Arraygröße: 2 0 0 Maraygröße: 2 0 0 Maraygröße: 2 0 0 Maraygröße: 0	
Quelle: Ja Senke: Ja Arraygröße: 1 C C Objektty: Arraygröße: 2 C C Arraygröße: 2 C C	
Senke: Ja AktivitätObjekte: Arraygröße: 1 C C Objekttyp: Arraygröße: 2 C C C	
AktivitätObjekte: Arraygröße: 1 C G 0: Objekttyp: Arraygröße: 2 C G G	
AktivitätObjekte: Arraygröße: 1 C 4 0: Objekttyp: Arraygröße: 2 C 4 im	
0: typ.dynamischesObjekt pid (Name: DynamischesObjekt) 📄	
1: typ.konfigurationsObjekt pid (Name: KonfigurationsObjekt) 📄	
Konfigurationsbereich: Arraygröße: 0 C D IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	
☑ ObjekteErzeugenÄndernLöschen	
AktivitätMengen:	
Arraygröße: 1 C	
U: [Mengentyp:	
Arraygröße: 0 C 🗇 📷	
Konfigurationsbereich:	
✓ MengeÄndern	
Rolle: Arraygröße: 0 0 🗘 🚭 📷	
aktuallar Datancata Datancata erzaugan Datancata läuskan Vasionen Piot	Fügen Cand

Abbildung 3-12: Parametrierung der Zugriffsrolle Adminstratoren



Die folgende Abbildung zeigt beispielhaft eine mögliche Versorgung von Operatoren. Diese wurde so parametriert, dass sämtliche Daten als einfacher Empfänger oder Sender angemeldet werden dürfen und dynamische Objekte vom Typ Meldung erzeugt bzw. gelöscht werden können.

• •	ParameterEditor
uswahl biekt: Operatoren	
ttributgruppe: Aktivitäten	Auswahl ändern
g.rollenAktivität:	
Urlasser:	
BenutzerReferenz: undefiniert	
Ursache: Defaultversorgung	
veraniasser:	
AktivitätDaten:	
Arraygröße: 1 C	
Name: GeneralEmptangerSender	
Arraygröße: 0 🗘 🖶 📷	
Attributaruppe:	
Arraygröße:	
Arraygrobe:	
Empfänger: Ja	0
Sender: Ja	
Quelle: Nein	
Senke: Nein	
AktivitätObjekte:	
Arraygröße: 1 C	
O:	
	nid (Name: Maldune) 🗎 🖨 🕞 🕞
Konfigurationsbereich	
Arraygröße:	
ObjekteErzeugenÄndernLöschen	
AktivitätMengen:	
Arraygröße: 1 🗘 🖶	
0: Mangentun:	
Arraygröße: 1 A	
U: menge.meidungen	pia 🔤 🐨 🔤 📃
Armurañe:	
Arraygroise: 0 V V	
✓ MengeÄndern	
Rolle:	
Arraygröße: 0 C 🖨 📷	
aktueller Datensatz Datensatz erzeugen E	Datensatz ioschen Kopieren Einfügen Senden

Abbildung 3-13: Parametrierung der Zugriffsrolle Operator



3.2.3.4 Region

Mit dem GTM werden alle Objekte vom Typ RegionNeu kontrolliert.

Objektty	′P	1 / 86	×	Þ	Objekte	1 / 1	×	Kappich
RegionNe	u (typ.zugriffsRegionNeu)				Gesamt (uz.schwelm.region.gesamt)			Systemberatung
RolleAlt (t	yp.zugriffsRolle)							integrativ und unabhängig Kompetens in System- und Verkehrstechnik
Simulation	(typ.zugriffskolleneu)							
	sverwartung (typ.sinitiationsverwartung)							Parameter editieren
Attribut	gruppe	1/4	×					Onlinetabelle anzeigen
Alternative Default-P	eObjektbezeichnung (atg.alternativeObjekt arameterdatensätze (atg.defaultParameter	bezeichnung) datensätze)						Konfigurationsdaten anzeigen
Info (atg.in Region (at	nfo) tg.region)			0				Aktuelle Daten anzeigen
								Aktuelle Daten senden
Aspekt		1/4	×					Archivanfrage (Stream)
Default-Pa Ist-Param	arameter-Aspekt (asp.parameterDefault)							
Soll-Parar	neter-Aspekt (asp.parameterSoll)							Systemprotokollierer starten
Vorgabe-	Parameter-Aspekt (asp.parameterVorgabe	:)						Systemplotokolilerer starten
								Onlineprotokollierer starten
Simulatio	nsvariante:	0	0					Datengenerator

Abbildung 3-14: Parametrierung der Regionen

In dem Tutorial ist nur die Region Gesamt versorgt, die alle Konfigurationsobjekte enthalten soll.

Abbildung 3-15 zeigt eine Möglichkeit, die Region Gesamt zu parametrieren. In diesem Fall erfolgt die Parametrierung der in der Region enthaltenen Objekte über die Option Bereiche. Dadurch, dass kein Konfigurationsverantwortlicher, Konfigurationsbereich und Typ vorgegeben wurden, greift hier der Wildcard-Mechanismus, was bedeutet, dass alle möglichen Konfigurationsobjekte in dem Bereich enthalten sind.



•	ParameterEditor
uswahl — bjekt: Gesamt ttributgruppe: Region	Auswahl ändern
g.region:	
BenutzerReferenz: undefiniert	
Ursache:	
Veranlasser:	
anthalteneObjekte:	
Arraygröße: 1 🗘 🖶	
0:	
Bereich:	
Arraygröße: 1 💭 👘	
Konfigurationsverantwortlicher:	
Arraygröße: 0 🗘 🖶 📷	
Konfigurationsbereich:	
Arraygröße: 0 🗘 🖶 📷	
Тур:	
Arraygröße: 0 🗘 🖶 📷	
Mengenbezeichnung:	
Region:	
Arraygröße: 0 🗘 🖶	
Objekte:	
Arraygröße: 0 🗘 🖶	
AusgeschlosseneObjekte:	
Arraygröße: 0 🗘 🖶	

Abbildung 3-15: Parametrierung der Region Gesamt



3.2.4 Einschaltung der Zugriffsrechteprüfung

Zur Aktivierung der Zugriffsrechteprüfung wird beim Datenverteiler der Aufrufparameter -rechtePruefung=neu⁶ gesetzt:

```
$java \
    -cp $distributionspakete/de.bsvrz.dav.dav/de.bsvrz.dav.dav-runtime.jar \
    -Xmx200m \
    de.bsvrz.dav.dav.main.Transmitter \
    -davAppPort=8083 -davDavPort=8082 -debugFilePath=.. \
    -rechtePruefung=nein \
    -warteAufParametrierung=nein \
    -datenverteilerId=1488439676845949071 \
    -benutzer=Standardapplikation \
    -konfigurationsBenutzer=configuration \
    -parametrierungBenutzer=parameter \
    -authentifizierung=passwd \
    -debugLevelStdErrText=INF0 \
    -debugLevelFileText=CONFIG \
    &
```

Danach wird das System gestartet.

Zur Kontrolle wird der GTM unter dem Benutzer Beobachter gestartet.

🔴 🔘 🔵 🛛 Kappich System	nberatung - Generischer Testmonitor - Login
Domainname / IP-Adresse:	localhost TCP-Portnummer: 8083 🔻
Benutzername:	Beobachter
Passwort:	•••••
(OK Beenden

Abbildung 3-16: GTM als Beobachter starten

Der Benutzer Beobachter meldet sich auf Datensätze der Attributgruppe StörfallZustand unter dem Aspekt StörfallVerfahrenStandard für den Messquerschnitt MQ.00 als Empfänger an. Dazu wird für die entsprechende Datenidentifikation eine Onlinetabelle geöffnet. Als initialen Datensatz wird in der Onlinetabelle "keine Daten (keine Quelle)" angezeigt, da für diese Datenidentifikation keine Quelle im Datenverteilersystem vorhanden ist.

⁶ Ab Version 3.13 der Kernsoftware wird unter dem Aufrufparameter -rechtePruefung=ja die neue Rechteprüfung aktiviert. Der Wert "neu" wird weiter unterstützt. Wenn die alte Rechteprüfung verwendet werden soll ist -rechtePruefung=alt zu setzen.



			StörfallZustand
Art	Zeit	Objekt	T Güte
			Index 4 Verfahren
OA 31.0	5.2019 13:00:19,519	MQ.00	keine Daten (keine Quelle)
1 31.0	5.2019 15.00.19,519	WIQ.00	Refire Daten (Refire Querie)

Abbildung 3-17: Anmeldung Empfänger StörfallZustand (als Beobachter)

Danach meldet sich der Benutzer Beobachter für die gleiche Datenidentifikation als Quelle an. Hierzu wird im GTM für die entsprechende Auswahl der Schalter "Aktuelle Daten senden" betätigt:

Datenidentifikatio	Aktuelle Daten senden - localhost:8083 onsauswahl
Attributgruppe:	StörfallZustand
Aspekt:	StörfallVerfahrenStandard
Objekt:	MQ.00
atg.störfallZusta	nd:
T: Undefinier	t
Situation: Un	definiert
Horizont: Un	definiert
Güte:	
Index: Und	efiniert
Verfahren:	Undefiniert_
Datensatz erz	eugen Datensatz löschen Datensatz senden
	Es liegen momentan keine Rechte für den Versand vor

Abbildung 3-18: Anmeldung Quelle StörfallZustand (als Beobachter)

Da die Zugriffsrechte des Benutzers Beobachter nur das Empfangen von Datensätzen zulässt, erhält er keine Sendesteuerung. Im GTM wird er über einen Tooltip darauf hingewiesen, dass die erforderlichen Rechte für diese Aktion nicht vorhanden sind.

Es wird ein weiterer GTM unter dem Benutzer Administrator gestartet:



Renutzername:	
benutzername.	Administrator
Passwort:	•••••
	OK Beenden

Abbildung 3-19: GTM als Administrator starten

Aus dieser Instanz des GTM erfolgt die Anmeldung als Quelle auf Datensätze der Attributgruppe StörfallZustand unter dem Aspekt StörfallVerfahrenStandard für den Messquerschnitt MQ.00.

tinbutgrup	pe. storranzustanu			
spekt:	StörfallVerfahrenStandard			
bjekt:	MQ.00			
g.störfallZ	ustand:			
T: 1 Minu	te			
Situation:	dichter Verkehr 🔹			
Horizont:	1 Stunde			
Güte:				
Index: 1	,0000			
Verfahren	: Standard			
Datensat	z erzeugen Datensatz löschen Datensatz senden			

Abbildung 3-20: Anmeldung Quelle StörfallZustand (als Administrator)

Die Daten werden in der Onlinetabelle des unter dem Benutzer Beobachter gestarteten GTM dargestellt:



Art			Storranzastana
	Zeit	Objekt	T Situation Horizont Cüte Cute Verfahren
OA 31.05.2	2019 13:00:19,519	MQ.00	keine Daten (keine Quelle)
OA 31.05.2	2019 13:05:30,294	MQ.00	keine Daten
OA 31.05.2	2019 13:06:15,228	MQ.00	1 Mdichter Verkehr 1 Stunde 1,0000 Standard

Abbildung 3-21: Onlinetabelle StörfallZustand (als Beobachter)

Im nächsten Schritt werden als Administrator die Zugriffsrechte des Benutzers Beobachter durch Änderung des Parameters Aktivitäten der Rolle Beobachter beschnitten.

Der Attributliste AktivitätDaten wird ein Feldeintrag hinzugefügt, der sämtliche Datenbefugnisse zur Attributgruppe StörfallZustand verbietet.

Dazu wird die Arraygröße zur AktivitätDaten auf 2 erhöht. Dem neuen Eintrag wird der Name "Ausnahme StörfallZustand" gegeben. In diesem Eintrag wird das Array zur Spezifikation der Attributgruppe auf 1 erhöht. Über den Schalter "Referenz ändern" wird ein Dialog geöffnet, über den die gewünschte Attributgruppe StörfallZustand ausgewählt wird.

Für den neuen Eintrag werden alle Datenbefugnisse (Empfänger, Sender, Quelle, Senke) auf "Nein" gesetzt.

Nachdem alle Eingaben getätigt wurden, wird der überarbeitete Parameterdatensatz über den Schalter "Senden" bestätigt. Die Parameteränderung wirkt sich sofort aus.

Straßen.NRW Tutorial

Zugriffsrechte Datenverteiler

Einstellung der Zugriffsrechte für ein fiktives Teilsystem



AktivitätDaten:	
Arraygröße: 2 🗘 🖶	
0:	
Name: GeneralEmpfänger	
Konfigurationsbereich:	
Arraygröße: 0 🗘 🖶 📷	
Attributgruppe:	
Arraygröße: 0 🗘 🖶 📷	
Aspekt:	
Arraygröße: 0 C 🖶 📷	
Empfänger: Ja	•
Sender: Nein	v
Quelle: Nein	
Senke: Nein	
1:	
Name: Ausnahme StörfallZustand	
Konfigurationsbereich:	
Arraygröße: 0 🗘 🖶 📷	
Attributgruppe:	
Arraygröße: 1 🗘 🖶 📷	
0: atg.störfallZustand pid (Nar	ne: StörfallZustand) 📄 🖶 🗟 📳 😑
Aspekt:	
Arraygröße: 0 C 🖶 📷	
Empfänger: Nein	•
Sender: Nein	▼
Quelle: Nein	•
Senke: Nein	v

Abbildung 3-22: Änderung der Aktivitäten zur Rolle Bebachter (als Administrator)



Als Resultat dieser Änderung wird in der Onlinetabelle, die unter dem Benutzer Beobachter gestartet wurde, der Datensatz "keine Daten, keine Rechte" ausgegeben:

			StörfallZustand
Art	Zeit	Objekt	T Situation Horizont Güte Index Verfahren
OA 31.0	5.2019 13:00:19,519	MQ.00	keine Daten (keine Quelle)
OA 31.0	5.2019 13:05:30,294	MQ.00	keine Daten
OA 31.0	5.2019 13:06:15,228	MQ.00	1 M dichter Verkehr 1 Stunde 1,0000 Standard
OA 31.0	5.2019 13:09:07,607	MQ.00	keine Daten (keine Rechte)
OA 31.0	5.2019 13:09:07,607	MQ.00	keine Daten (keine Rechte)

Abbildung 3-23: Onlinetabelle StörfallZustand entzogene Rechte (als Beobachter)

Danach wird die Parameteränderung wieder rückgängig gemacht. Als Resultat wird in der Onlinetabelle, die unter dem Benutzer Beobachter gestartet wurde, der letzte Datensatz wieder ausgegeben, da nun die Einschränkung nicht mehr gilt.

						StörfallZu	istand				
Art	Zeit	Objekt	T∢	T Situation Horizont		Güte	-				
24 21 (25 2010 12:00:10 510		kaina	Datan (kaina	0		Index	 Verfahren 	-		
OA 31.0	5.2019 13:00:19,519	MQ.00	Keine	keine Daten (keine Quelle)							
OA 31.0	05.2019 13:05:30,294	MQ.00	Keine	Daten							
OA 31.0	05.2019 13:06:15,228	MQ.00	1 M d	ichter Verkehr		1 Stunde	1,0000	Standard			
OA 31.0	05.2019 13:09:07,607	MQ.00	keine	Daten (keine	Rech	te)					
OA 31.0	05.2019 13:06:15,228	MQ.00	1 M d	ichter Verkehr		1 Stunde	1,0000	Standard			
OA 31.0	05.2019 13:06:15,228	MQ.00	1 M d	ichter Verkehr		1 Stunde	1,0000	Standard	_		

Abbildung 3-24: Onlinetabelle StörfallZustand (wieder) erteilte Rechte (als Beobachter)



3.2.5 Darstellung der Rechte mit dem GTM

Seit Version 3.13 der Kernsoftware können die Zugriffsberechtigungen eines Benutzers im GTM eingeblendet werden.

Dazu muss im Menü "Ansicht" im Untermenü "Berechtigungen" zum einen "Berechtigungen anzeigen" und zum anderen im weiteren Untermenü "Berechtigungen für Benutzer" der Benutzer ausgewählt werden.



Abbildung 3-25: GTM Menü Ansicht

Danach werden die parametrierten Berechtigungen in der Objekteliste je Objekt eingeblendet. Über einen Tooltipp werden Angaben zum Objekt sowie zu den Einstellungen ausgegeben.



Abbildung 3-26: Onlinetabelle StörfallZustand (als Beobachter)



3.3 Kopplung zweier Datenverteilersysteme

Die UZ Schwelm soll mit einem weiteren Datenverteilersystem, der fiktiven autarken Organisationseinheit UZ Ennepetal, gekoppelt werden.



Abbildung 3-27: Kopplung zweier Datenverteilersysteme

Hierzu muss eine Datenverteiler-Datenverteiler-Verbindung versorgt und parametriert werden. Es muss ein Konfigurationsobjekt vom Typ typ.datenverteilerVerbindung angelegt werden. Im konfigurierenden Datensatz zur Attributgruppe atg.datenverteilerTopologie muss die Kommunikationstopologie der Datenverteiler definiert werden. Für die Einrichtung der Zugriffsrechte sind dabei folgende Punkte wichtig:

- Je Datenverteiler-Datenverteiler-Verbindung muss ein Verbindungsobjekt definiert sein.
- Die beteiligten Datenverteiler müssen angegeben werden (Referenzen auf die entsprechenden Datenverteilerobjekte)
- Die Datenverteiler müssen sich beim Verbindungsaufbau gegeneinander authentifizieren. Dazu müssen die Namen der Benutzer angegeben werden, mit dem sich der eine Datenverteiler jeweils beim anderen Datenverteiler authentifiziert.

Die erforderlichen Informationen sind an Objekte gebunden. Damit muss die Frage geklärt werden, welches Objekt in welchem System konfiguriert bzw. parametriert werden soll.

Abbildung 3-28 skizziert die Informationen, die eine Datenverteilerverbindung bezüglich der Zugriffsrechte aufweisen muss. Das Verbindungsobjekt "UZ Schwelm UZ Ennepetal" mit der PID davDav.uz.schwelm.uz.ennepetal definiert eine Verbindung, die zwischen dem Datenverteiler der UZ Schwelm (PID dav.uz.schwelm) und dem Datenverteiler der UZ Ennepetal (dav.uz.ennepetal) aufgebaut werden soll. Dabei soll die Verbindung aktiv von der UZ Ennepetal aufgebaut werden. Der Benutzer, unter dem sich der Datenverteiler der UZ Schwelm beim Verbindungsaufbau gegenüber der UZ Ennepetal authentifiziert, hat den Namen SchwelmRechteInEnnepetal und die PID uz.ennepetal.benutzer.uz.schwelm.



	UZ Schwelm UZ Ennepetal
	(davDaV.uz.schwelm.uz.ennepetal)
\bigcirc	UZ Schwelm
\bigcirc	(dav.uz.schwelm)
\bigtriangledown	UZ Ennepetal
\sim	(dav.uz.ennepetal)
	schwelmRechteInEnnepetal
	(uz.ennepetal.benutzer.uz.schwelm)
	ennepetalRechteInSchwelm
	(uz.schwelm.benutzer.uz.ennepetal)

Abbildung 3-28: Datenverteilerverbindungsobjekt

Abbildung 3-29 enthält die zu konfigurierenden und parametrierenden Objekte für die Datenverteilerverbindung. Dabei sind die Objekte jeweils im Bereich der zuständigen UZ eingetragen.

Die UZ Schwelm soll für die Datenverteilerverbindung zuständig sein. Deshalb wurde das Datenverteilerverbindungsobjekt (davDav.uz.schwelm.uz.ennepetal) hier konfiguriert. Welche Zugriffsrechte die UZ Ennepetal gegenüber der UZ Schwelm hat, muss natürlich in der AOE der UZ Schwelm festgelegt werden. Deshalb muss der Benutzer, unter dem sich der Datenverteiler der UZ Ennepetal authentifiziert, in der UZ Schwelm parametriert werden.



Abbildung 3-29: Kopplung zweier Datenverteilersysteme

Damit die Konfiguration der UZ Schwelm erstellt werden kann, muss von der UZ Ennepetal der Konfigurationsbereich übernommen werden, in dem das Datenverteilerobjekt der UZ Ennepetal definiert wurde. Dieses Objekt wird ja im konfigurierenden Datensatz zur Datenverteilerverbindung referenziert.

Nachdem die Objekte zur Datenverteilerverbindung bei der UZ Schwelm erstellt wurden, müssen der UZ Ennepetal die erforderlichen Konfigurationsbereiche zur Verfügung gestellt werden.

Der Ablauf zur Erstellung einer Datenverteilerverbindung soll in den folgenden Unterpunkten noch einmal skizziert werden.



3.3.1 Konfiguration der Datenverteilerverbindung

3.3.1.1 UZ Ennepetal

Für die UZ Ennepetal wurde bereits ein Datenverteilerobjekt versorgt. Der Datenverteiler hat in dem Beispiel als IP-Adresse localhost und als Port 8084. Unter diesen Parametern akzeptiert der Datenverteiler Verbindungen zu anderen Datenverteilern.

```
<konfigurationsObjekt pid="dav.uz.ennepetal"

name="Datenverteiler UZ Ennepetal"

typ="typ.datenverteiler">

<info>

<kurzinfo>Datenverteiler</kurzinfo>

</info>

<datensatz attributgruppe="atg.datenverteilerEigenschaften"

aspekt="asp.eigenschaften">

<datum name="adresse" wert="localhost"/>

<datum name="subAdresse" wert="8084"/>

</datensatz>

<objektMenge name="Applikationen">

</konfigurationsObjekt>
```

Abbildung 3-30: Versorgung Datenverteiler dav.uz.ennepetal

Für die Datenverteilerverbindung zur UZ Schwelm stellt die UZ Ennepetal einen Benutzer zur Verfügung (SchwelmRechteInEnnepetal), unter dem sich der Datenverteiler der UZ Schwelm beim Aufbau der Datenverteilerverbindung authentifizieren muss. Die Parametrierung der Zugriffsrechte für diesen Benutzer findet auf der UZ Ennepetal statt. Im Beispiel wurde diesem Benutzer auf der UZ Ennepetal später die Berechtigungsklasse Beobachter zugewiesen.

Abbildung 3-31: Versorgung Benutzer uz.ennepetal.benutzer.uz.schwelm

Die UZ Ennepetal muss dafür Sorge tragen, dass das Passwort, unter dem sich der Datenverteiler der UZ Schwelm gegenüber dem Datenverteiler der UZ Ennepetal authentifiziert in der Benutzerverwaltungsdatei der Konfiguration der UZ Ennepetal befindet.

</benutzerkonten>

Abbildung 3-32: Benutzerverwaltung UZ Ennepetal (Auszug Datei benutzerverwaltung.xml)



Achtung: Das entsprechende Passwort muss in der Passwortdatei stehen, die der Datenverteiler der UZ Schwelm als Aufrufargument (-authentifizierung=passwd) gesetzt hat.

configuration=SRP6~~~~ 23c33c3392177514ba113c5105c894e3640c80e9bcce82db27525b7ec7.... parameter=SRP6~~~~ 670ce5faa22ecc290046d648f8c00e89df664230565907cb5cb56ae5cae9a8.... Standardapplikation=SRP6~~~~ 861008a6a98f7d3d2126f0690b7a97823906a41919f6a628738d.... SchwelmRechteInEnnepetal=SRP6~~~ e991d387f6f41545872d0e7b855e898946708b32abc6e64....

Abbildung 3-33: Auszug <code>passwd</code> UZ Schwelm

Für die Authentifizierung der Datenverteiler untereinander muss natürlich bei der UZ Schwelm das Passwort, unter dem sich der Datenverteiler der UZ Ennepetal authentifiziert in der Benutzerverwaltung der UZ Schwelm aufgeführt sein und in der passd Datei das Passwort, mit dem sich der Datenverteiler der UZ Schwelm gegenüber dem Datenverteiler der UZ Ennepetal authentifiziert (also EnnepetalRechteInSchwelm).

3.3.1.2 UZ Schwelm

Für die UZ Schwelm wurde bereits ein Datenverteilerobjekt versorgt. Der Datenverteiler hat in dem Beispiel als IP-Adresse localhost und als Port 8082. Unter diesen Parametern akzeptiert der Datenverteiler Verbindungen zu anderen Datenverteilern.

Abbildung 3-34: Versorgung Datenverteiler dav.uz.schwelm

Das Datenverteilerverbindungsobjekt wird auf der UZ Schwelm folgendermaßen versorgt. Damit dieses Konfigurationsobjekt in der Konfiguration der UZ Schwelm angelegt werden kann, muss diese Konfiguration vorher die Konfigurationsbereiche von der UZ Ennepetal übernehmen, die bei der Erstellung des Datenverteilerobjektes dav.uz.ennepetal involviert waren.

Straßen.NRW

Tutorial Zugriffsrechte Datenverteiler Einstellung der Zugriffsrechte für ein fiktives Teilsystem



```
<!-- Verbindung zwischen DaV UZ Schwelm und UZ Ennepetal -->
<konfigurationsObjekt pid="davDaV.uz.schwelm.uz.ennepetal"
                      typ="typ.datenverteilerVerbindung">
  <info>
      <kurzinfo>
          Verbindung zwischen UZ Schwelm und UZ Ennepetal,
          wird von UZ Ennepetal aufgebaut.
      </kurzinfo>
  </info>
  <datensatz attributgruppe="atg.datenverteilerTopologie" aspekt="asp.eigenschaften">
      <datum name="datenverteilerA" wert="dav.uz.schwelm"/>
      <datum name="datenverteilerB" wert="dav.uz.ennepetal"/>
      <datum name="wichtung" wert="1"/>
      <datum name="aktiverDatenverteiler" wert="B"/>
      <datum name="ersatzverbindungsWartezeit" wert="1 Minute"/>
      <datum name="benutzer1" wert="SchwelmRechteInEnnepetal"/>
      <datum name="benutzer2" wert="EnnepetalRechteInSchwelm"/>
      <datenliste name="durchsatzPrüfung">
          <datum name="pufferFüllgrad" wert="75 %"/>
          <datum name="prüfIntervall" wert="3 Minuten"/>
          <datum name="mindestDurchsatz" wert="3000 Byte/s"/>
      </datenliste>
  </datensatz>
  <objektMenge name="Ersatzverbindungen">
  </objektMenge>
</konfigurationsObjekt>
```

Abbildung 3-35: Versorgung Datenverteilerverbindung davDaV.uz.schwelm.uz.ennepetal

Der konfigurierende Datensatz zur Datenverteilertopologie gibt an, dass eine Datenverteilerverbindung zwischen dem Datenverteiler A dav.uz.schwelm und dem Datenverteiler B dav.uz.ennepetal aufgebaut werden soll, wobei der Datenverteiler B der aktive Datenverteiler ist, also die Verbindung aufbaut. Unter den Feldern benutzer1/2 werden die Benutzer angegeben, unter denen sich der jeweilige Datenverteiler beim anderen authentifiziert. Die weiteren Einträge in dem konfigurierenden Datensatz sind für die Zugriffsrechte nicht relevant.

Für die Datenverteilerverbindung zur UZ Ennepetal stellt die UZ Schwelm einen Benutzer zur Verfügung (EnnepetalRechteInSchwelm), unter dem sich der Datenverteiler der UZ Ennepetal beim Aufbau der Datenverteilerverbindung authentifizieren muss. Die Parametrierung der Zugriffsrechte für diesen Benutzer findet auf der UZ Schwelm statt. In der Parametrierung wird diesem Benutzer die Berechtigungsklasse EnnepetalRechteInSchwelm zugewiesen.

Abbildung 3-36: Versorgung Benutzer uz.schwelm.benutzer.uz.ennepetal



Kontrolle der Parametrierung der Zugriffsrechte für die DaV-DaV-Verbindung

Param	eterEditor
Auswahl Dbjekt: EnnepetalRechteInSchwelm Attributgruppe: Berechtigungsklassen	Auswahl ändern
g.berechtigungsklassen: Urlasser: BenutzerReferenz: undefiniert Ursache:	
Berechtigungsklassen: Arraygröße: 1 2 4 📷 0: uz.schwelm.berechtigungsklasse.uz.ennepetal	pid (Name: EnnepetalRechtelnSchwelm) 🚞 🝚 📷 💼 😑
aktueller Datensatz Datensatz erzeugen Date	nsatz löschen Kopieren Einfügen Senden

Abbildung 3-37: Parametrierung Benutzer "EnnepetalRechteInSchwelm"

Die Berechtigungsklasse EnnepetalRechteInSchwelm wird aus den extra für die DaV-DaV-Verbindung neuen Rolle und Region gebildet. Damit könnten später detailliert die Rechte, die für die UZ Ennepetal in der UZ Schwelm gelten eingestellt werden.

ttributgruppe: RollenRegionenPaare	Auswahl ändern
g.rollenRegionenPaare:	
Urlasser:	
BenutzerReferenz: undefiniert	
Ursache:	
Veranlasser:	
RollenRegionenPaare:	
Arraygröße: 1 🔒 🖨	
0.	
Rolle: uz schweim rolle uz ennenetal	nid (Name: EnnenetalRechtelnSchwelm)
Pagion: uz schwelm region uz ennenetal	nid (Name: EnnepetalRechteinSchweim)
kegion. uz.schweim.region.uz.ennepetai	
aktueller Datensatz	Datensatz löschen Kopieren Finfügen Senden

Abbildung 3-38: Parametrierung Berechtigungsklasse "EnnepetalRechteInSchwelm"



Auswahl							
Objekt: EnnepetalRechteInSchwelm	ahländern						
Attributgruppe: Aktivitäten							
tg.rollenAktivität:							
Urlasser:							
BenutzerReferenz: undefiniert							
Ursache: Defaultversorgung							
Veranlasser:							
AktivitätDaten:							
Arraygröße: 1 🗘 🖶							
0:							
Name: GeneralEmpfänger							
Konfigurationsbereich:							
Arraygröße: 0 C 🖶 📷							
Attributgruppe:							
Arraygröße: 0 🗘 🖶 📷							
Aspekt:							
Arraygröße: 0 🗘 🖶 📷							
Empfänger: Ja	$\overline{\mathbf{O}}$						
Sender: Nein	<u> </u>						
Quelle: Nein	<u></u>						
Senke: Nein	<u></u>						
AktivitätObjekte:							
Arraygröße: 0 🗘 🖶							
AktivitätMengen:							
Arraygröße: 0							
Rolle:							
Arraygröße: 0 🗘 🖶 📷							

Abbildung 3-39: Parametrierung Aktivitäten "EnnepetalRechteInSchwelm"



Die Region kann über den GTM kontrolliert und angepasst werden. Abbildung 3-40 zeigt den Fall, dass über die Datenverteilerverbindung von der UZ Ennepetal grundsätzlich zu allen Objekten aus dem Konfiguration der UZ Schwelm Aktivitäten durchgeführt werden dürfen.

•	Farametercultur
uswahl	
tributaruppe: Pagion	Auswahl ändern
J.region:	
Irlasser:	
BenutzerReferenz: undefiniert	
Ursache:	
veranlasser:	
nthalteneObjekte:	
Arraygröße: 1 C	
O:	
Konfigurationsverantwortlicher:	
Arraygröße: 0 🗘 🖶 📷	
Konfigurationsbereich:	
Arraygröße: 0 🗘 🖨 📷	
Arraygröße: 0 🗘 🖶 📷	
Mengenhezeichnung	
Mengenbezeichnung.	
- Pegion:	
Arraygröße: 0 C	
Objekte:	
usgeschlosseneObjekte:	
Arraygröße: 0 🗘 🖶	

Abbildung 3-40: Parametrierung Region EnnepetalRechteInSchwelm



3.3.2 Start der Systeme

Nachdem die beiden Datenverteilersysteme ordnungsgemäß konfiguriert und parametriert wurden, können sie beide gestartet werden.

Der Datenverteiler der UZ Ennepetal versucht nach einer vorgegebenen Zeitspanne eine Verbindung zum Datenverteiler der UZ Schwelm aufzubauen. Nach der erfolgreichen Authentifizierung der beiden Datenverteiler können richtungsabhängig die entsprechend mit den Zugriffsrechten der jeweiligen Seite vereinbarten Daten ausgetauscht werden.

Ob die DaV-DaV-Verbindung hergestellt werden konnte, kann z.B. in der Debugdatei des Datenverteilers bei der UZ Schwelm kontrolliert werden:

Nach einer Wartezeit lässt der Datenverteiler Verbindungen von und zu anderen Datenverteilern zu.

#000026 31.05.2019 18:05:39,826:+0200 (TID:000001) ------INFO : Datenverteiler.de.bsvrz.dav.dav.main.Transmitter Datenverteiler bereit

Hier baut der Datenverteiler der UZ Ennepetal eine Verbindung zum Datenverteilern der UZ Schwelm auf (nach Port 8082 DaV-Port der UZ Schwelm).

#000027 31.05.2019 18:05:59,684:+0200 (TID:000072) ------INF0 : Datenverteiler.de.bsvrz.dav.daf.communication.tcpCommunication.TCP_IP_ServerCommunication TCP-Verbindung passiv aufgebaut, /127.0.0.1:8082 <-- /127.0.0.1:50461</pre>

Verbundene Datenver Datenverteiler	rteiler vor Adresse	dav.uz.schwelm: Zustand	Verschlüsselung	Meldung
dav.uz.ennepetal		Warte auf eingehende Verbindung	Nicht verschlüsselt	

#000029 31.05.2019 18:05:59,724:+0200 (TID:000075) --------INFO : Datenverteiler.de.bsvrz.dav.dav.communication.davProtocol.T_T_HighLevelCommunication Verschlüsselung der Verbindung wird deaktiviert

Der Datenverteiler der UZ Ennepetal authentifiziert sich der bei der UZ Schwelm.

#000030 31.05.2019 18:05:59,725:+0200 (TID:000075) ------INF0 : Datenverteiler.de.bsvrz.dav.communication.davProtocol.T_T_HighLevelCommunication Datenverteiler 1490691476659634301 möchte sich authentifizieren

#000031 31.05.2019 18:05:59,726:+0200 (TID:000075) ------INFO : Datenverteiler.de.bsvrz.dav.dav.communication.davProtocol.T_T_HighLevelCommunication Datenverteiler 1490691476659634301 hat sich als 'EnnepetalRechteInSchwelm' erfolgreich authentifiziert

Verbundene Datenver	teiler von dav.uz.	schwelm:		
Datenverteiler	Adresse	Zustand	Verschlüsselung	Meldung
dav.uz.ennepetal	localhost:50461	Authentifizierung	Nicht verschlüsselt	
#000033 31.05.2019 INF0 : Datenverte	18:05:59,744:+0200 eiler.de.bsvrz.dav.) (TID:000014) dav.main.DebugTransm	nitterPublisher	
Verbundene Datenver	<pre>rteiler von dav.uz.</pre>	schwelm:		
Datenverteiler	Adresse	Zustand	Verschlüsselung	Meldung
dav.uz.ennepetal	localhost:50461	Verbunden	Nicht verschlüsselt	

Die zustanden gekommene Verbindung wird in der Debug-Datei ausgegeben. Die Datenverteiler-Datenverteiler-Verbindung wird hier übrigens deshalb nicht verschlüsselt, weil die beiden



Systeme im Beispiel auf einem Rechner laufen. Hier wird per Default keine Verschlüsselung durchgeführt.

3.3.3 Einstellung der Zugriffsrechte zwischen Datenverteilern

Die Einstellung der Zugriffsrechte zwischen zwei Datenverteilern erfolgt analog zu der Einstellung der Zugriffsrechte für eine einfache Applikation. Dabei ist zu beachten, dass die Zugriffsrechte von Benutzern innerhalb eines Systems durch die Datenverteilerverbindung weiter eingeschränkt werden können.



Abbildung 3-41: Beispielszenario Datenverteilerverbindung

Abbildung 3-41 skizziert ein etwas erweitertes Szenario der Verbindung zwischen der UZ Schwelm und der UZ Ennepetal. Bei der UZ Ennepetal läuft die Applikation App_j, die unter dem Benutzer A gestartet wurde. Dieser Benutzer wird im System der UZ Ennepetal verwaltet und hat alle möglichen Rechte (grün ausgefüllter Berechtigungsraum). Der Datenverteiler der UZ Ennepetal authentifiziert sich unter dem Benutzer B gegenüber dem Datenverteiler der UZ Schwelm. Die Zugriffsrechte der Benutzer B werden auf der UZ Schwelm verwaltet. Dabei ist hier im Berechtigungsraum der obere Bereich nicht erlaubt.

Wenn die Applikation App_j beim Datenverteiler Datensätze zu den skizzierten Objekten O_k und O_i als Empfänger anmeldet, und die Daten zu O_k von der Applikation App_k im System der UZ Ennepetal und die Daten zu O_i von der Applikation App_i im System der UZ Schwelm erzeugt werden, passiert folgendes: die Datensätze zu O_k werden direkt an App_j geliefert. Die Datensätze zu O_i werden nicht an App_j geliefert, da diese Datensätze nicht in dieser Richtung über die Datenverteilerverbindung übertragen werden dürfen. Damit werden die Zugriffsrechte des Benutzers A für Daten aus System UZ Schwelm entsprechend der Abbildung beschnitten.



3.3.4 Beispiel

Ein Benutzer **X** hat auf der UZ Ennepetal Administratorrechte und darf dementsprechend mit allen Daten arbeiten.

Zum Beispiel meldet sich der Benutzer X für die Attributgruppe VerkehrsdatenkurzeitMQ unter dem Aspekt Analyse der Messquerschnitte MQ.00, MQ.01 und MQ.03 der UZ Schwelm bei der UZ Ennepetal an.

Wenn die Datenverteilerverbindung zur UZ Schwelm noch nicht steht oder noch keine Quelle für die Daten auf der UZ Schwelm zur Verfügung steht, erhält der Benutzer X den Ergebnisdatensatz "keine Daten (keine Quelle)".



Abbildung 3-42: Anmeldung bei der UZ Ennepetal auf Daten der UZ Schwelm

Wenn sich, wie im Beispiel nachgestellt, die Applikation auf der UZ Schwelm gestartet wird, wird zu den angemeldeten Daten zunächst der Datensatz "keine Daten" publiziert, da nun eine Quelle zur Verfügung steht; diese aber noch keine Daten geliefert hat. In Folge werden die generierten Daten der Applikation zu den MQ erzeugt.



Diese Datensätze werden auch über die DaV-DaV-Verbindung zur UZ Ennepetal übertragen und der Benutzer **X** kann darauf zugreifen, wie in der folgenden Abbildung im GTM dargestellt ist.

							C)Kfz			
Art Zeit	Zeit	Objekt				Status					
			W4	Erfassung 4	PIFormal 4		PlLogisch		 MessWertEr 		
				NichtErfa∢	Wert 4	Wert∢	WertMaxLogi∢	WertMinLogi	Implausi		
)A	31.05.2019 18:47:59,670	MQ.00	keine	Daten (keine (Quelle)						
)A	31.05.2019 18:47:59,670	MQ.01	keine	keine Daten (keine Quelle)							
DA :	31.05.2019 18:47:59,670	MQ.02	keine	keine Daten (keine Quelle)							
DA	31.05.2019 18:53:12,460	MQ.00	keine	keine Daten							
DA :	31.05.2019 18:53:12,460	MQ.01	keine								
DA :	31.05.2019 18:53:12,460	MQ.02	keine	keine Daten							
)A	31.05.2019 18:54:00,000	MQ.00	8250	Ja	Nein	Nein	Ja	Ja	Ja		
A	31.05.2019 18:54:00,000	MQ.01	2935	Ja	Nein	Nein	Nein	Ja	Ja		
A	31.05.2019 18:54:00,000	MQ.02	4414	Ja	Nein	Ja	Nein	Nein	Nein		
A	31.05.2019 18:55:00,000	MQ.00	3298	Ja	Nein	Nein	Ja	Nein	Ja		
)A	31.05.2019 18:55:00,000	MQ.01	5493	Nein	Nein	Nein	Ja	Nein	Ja		
DA :	31.05.2019 18:55:00,000	MQ.02	5026	Ja	Nein	Nein	Ja	Ja	Nein		
DA :	31.05.2019 18:56:00,000	MQ.00	2673	Ja	Ja	Nein	Ja	Ja	Ja		
DA :	31.05.2019 18:56:00,000	MQ.01	4202	Ja	Nein	Ja	Ja	Ja	Ja		
24	31.05.2019 18:56:00.000	MO.02	1867	Nein	Ja	Ja	Ja	Nein	Nein		

Abbildung 3-43: Daten zu den MQ der UZ Schwelm für Benutzer X

Der über die DaV-DaV-Verbindung zulässige Datenaustausch kann auf beiden Seiten beschränkt werden.

Im Beispiel wird bei den Zugriffsrechten, die die UZ Ennepetal gegenüber der UZ Schwelm hat, die Region in der Form geändert, dass von der UZ Schwelm zur UZ Ennepetal grundsätzlich keine Daten mehr zu dem Messquerschnitt MQ.00 erlaubt sind und damit auch nicht mehr über die DaV-DaV-Verbindung übertragen werden.

Diese Änderung wird durchgeführt, indem in der Parametrierung der UZ Schwelm der Parameterdatensatz zur Attributgruppe Region zum Objekt EnnepetalRechteInSchwelm vom Typ RegionNeu bei den ausgeschlossenen Objekten das entsprechende Objekt MQ.00 (PID uz.schwelm.mq.00) eingetragen und gesendet wird (s. Abbildung 3-44).



uswani bjekt: EnnepetalRechtelnSchwelm ttributgruppe: Region	Auswahl ändern
g.region:	
Urlasser:	
BenutzerReferenz: undefiniert	
Ursache:	
Veranlasser:	
EnthalteneObjekte:	
Arraygröße: 1 C 🖶	
Bereich:	
Arraygröße: 1 🗘 📮	
℃	
Konfigurationsverantwortlicher:	
Arraygröße: 0 C 🖶 📷	
Konfigurationsbereich:	
Arraygröße: 0 🗘 🖶 📷	
Тур:	
Arraygröße: 0 🗘 🖶 📷	
Mengenbezeichnung:	
	₽ III =
Region:	
Arraygröße: 0 🗘 🖶	
Objekte:	
Arraygröße: 0 🗘 🖶	
Ausaeschlassene0hiekte	
Arravoröße:	
0:	
Bereich:	
Arraygröße: 0 🗘 🖨	
Region:	
Arraygröße: 0 🗘 🖨	
Objekte:	
Arraygröße: 1 🗘 🖨	
0:	
Objekt:	
Arraygroße: 1 😳 😭 📷	
U: uz.schweim.mq.00	pid (Name: MQ.00) 📄 😭 📾 🗐 📟
Mengenbezeichnung:	
aktueller Datensatz Datensatz erzeugen Date	ensatz löschen Kopieren Einfügen Senden

Abbildung 3-44: Einschränkung der Zugriffsrechte für Ennepetal auf Daten in Schwelm

Diese Einschränkung wirkt sich direkt auf den Benutzer **X** aus, da die von ihm angemeldeten Daten nicht mehr über die DaV-DaV-Verbindung in Richtung UZ Ennepetal übertragen werden.



Der Benutzer **X** erhält zur Information für die angemeldete Datenidentifikation den Datensatz "Keine Daten (Keine Rechte).

•		Onlinetabelle (Attributgru	ppe: Ve	erkehrsDatenKu	ırzZeitMq,	Aspekt: Ar	alyse) - localhost:	8085		
							(QKfz		-
Art	Zeit	Objekt					Status			
			W∢	Erfassung 4	PIFormal 4		PlLogisch 4		MessWertEr	
				NichtErfa∢	Wert 4	Wert ∢	WertMaxLogi∢	WertMinLogi ◀	Implausi	1
OA	31.05.2019 18:53:12,460	MQ.01	keine							
OA	31.05.2019 18:53:12,460	MQ.02	keine							
OA	31.05.2019 18:54:00,000	MQ.00	8250	Ja	Nein	Nein	Ja	Ja	Ja	N
OA	31.05.2019 18:54:00,000	MQ.01	2935	Ja	Nein	Nein	Nein	Ja	Ja	J
OA	31.05.2019 18:54:00,000	MQ.02	4414	Ja	Nein	Ja	Nein	Nein	Nein	Ţ
OA	31.05.2019 18:55:00,000	MQ.00	3298	Ja	Nein	Nein	Ja	Nein	Ja	J
OA	31.05.2019 18:55:00,000	MQ.01	5493	Nein	Nein	Nein	Ja	Nein	Ja	T
OA	31.05.2019 18:55:00,000	MQ.02	5026	Ja	Nein	Nein	Ja	Ja	Nein	Ţ
OA	31.05.2019 18:56:00,000	MQ.00	2673	Ja	Ja	Nein	Ja	Ja	Ja	Ţ
OA	31.05.2019 18:56:00,000	MQ.01	4202	Ja	Nein	Ja	Ja	Ja	Ja	T
DA	31.05.2019 18:56:00,000	MQ.02	1867	Nein	Ja	Ja	Ja	Nein	Nein	Ţ
OA	31.05.2019 18:57:00,000	MQ.00	2227	Nein	Ja	Nein	Ja	Nein	Ja	Ţ
OA	31.05.2019 18:57:00,000	MQ.01	8161	Nein	Nein	Ja	Nein	Ja	Ja	Ţ
OA	31.05.2019 18:57:00,000	MQ.02	3044	Nein	Nein	Ja	Ja	Nein	Ja	Ţ
OA	31.05.2019 18:57:33,917	MQ.00	keine	Daten (keine l	Rechte)					
OA	31.05.2019 18:58:00,000	MQ.01	6402	Nein	Ja	Ja	Nein	Nein	Ja	Ţ
OA	31.05.2019 18:58:00,000	MQ.02	7275	Ja	Ja	Nein	Nein	Ja	Nein	T

Abbildung 3-45: Auswirkung der Einschränkung für Benutzer X

Wenn auf der Seite der UZ Schwelm die Ausnahme wieder zurückgenommen wird, werden die Daten wieder über die Datenverteiler-Datenverteiler-Verbindung übertragen und stehen somit direkt wieder zur Verfügung.

			L	nr			L L	ĮKTZ		_
Art	rt Zeit	Objekt					Status		1	
			₩∢	Erfassung ∢	PIFormal 4		PILogisch 4		MessWertErs	
				NichtErfa∢	Wert 4	Wert 4	WertMaxLogi∢	WertMinLogi ∢	Implausi4	Į.
OA	31.05.2019 18:55:00,000	MQ.00	3298	Ja	Nein	Nein	Ja	Nein	Ja	Ja
OA	31.05.2019 18:55:00,000	MQ.01	5493	Nein	Nein	Nein	Ja	Nein	Ja	N
OA	31.05.2019 18:55:00,000	MQ.02	5026	Ja	Nein	Nein	Ja	Ja	Nein	Ja
OA	31.05.2019 18:56:00,000	MQ.00	2673	Ja	Ja	Nein	Ja	Ja	Ja	Ja
OA	31.05.2019 18:56:00,000	MQ.01	4202	Ja	Nein	Ja	Ja	Ja	Ja	N
OA	31.05.2019 18:56:00,000	MQ.02	1867	Nein	Ja	Ja	Ja	Nein	Nein	Ja
OA	31.05.2019 18:57:00,000	MQ.00	2227	Nein	Ja	Nein	Ja	Nein	Ja	Ja
OA	31.05.2019 18:57:00,000	MQ.01	8161	Nein	Nein	Ja	Nein	Ja	Ja	Ja
OA	31.05.2019 18:57:00,000	MQ.02	3044	Nein	Nein	Ja	Ja	Nein	Ja	Ja
OA	31.05.2019 18:57:33,917	MQ.00	keine							
OA	31.05.2019 18:58:00,000	MQ.01	6402	Nein	Ja	Ja	Nein	Nein	Ja	Ja
OA	31.05.2019 18:58:00,000	MQ.02	7275	Ja	Ja	Nein	Nein	Ja	Nein	N
OA	31.05.2019 18:59:00,000	MQ.01	5128	Nein	Nein	Nein	Ja	Ja	Nein	Ja
OA	31.05.2019 18:59:00,000	MQ.02	8476	Ja	Nein	Nein	Ja	Ja	Ja	Ja
OA	31.05.2019 19:00:00,000	MQ.01	7466	Ja	Nein	Ja	Nein	Ja	Nein	Ja
OA	31.05.2019 19:00:00,000	MQ.02	nicht	. Ja	Nein	Nein	Nein	Ja	Ja	N
OA	31.05.2019 19:00:00,000	MQ.00	4572	Nein	Ja	Ja	Ja	Nein	Ja	N

Abbildung 3-46: Auswirkung Rücknahme der Einschränkung für Benutzer X