von Willy Günther

Mit dieser neuen Funktion bekommen wir die Möglichkeit, die Zugriffe die eine Anwendung ausführt, und die Sicherheitsüberprüfungen die vom System durchgeführt werden, aufzuzeichnen. Damit sehe ich welche Zugriffsrechte benötigt werden, und ich sehe auch welche Zugriffsrechte das Benutzer Profil verwendet, das auf die Anwendung bzw. die Datenbank zugreift. Dadurch lässt sich feststellen, ob ein Benutzer mehr Rechte besitzt als er für seine Aufgaben benötigt. Damit ist eine Optimierung der Zugriffsrechte möglich, die sicherstellt, dass die erforderlichen Rechte vorhanden sind aber der Benutzer nicht unnötige Rechte besitzt.
Durch das Aufzeichnen der Zugriffe kann ich auch feststellen auf welche Objekte die Anwendung / der Benutzer zugreift.

Das Tool dokumentiert aber nicht alle Zugriffsrechte. Special Authorities wie z. B. *JOBCTL oder *SAVSYS generieren keine Einträge. Betriebssystem Objekte die in der *SYSTEM Domain laufen oder Objekte in der QTEMP oder QSPL werden nicht aufgezeichnet. Mehr Details zu den Ausnahmen finden Sie hier:

https://ibm.biz/Bdjac8

Mit der Authority Collection kann ich die Zugriffe und die vorhanden bzw. erforderlichen Zugriffsrechte dokumentieren und dem Security Verantwortlichen zur Verfügung stellen. Das Tool macht keine Vorgaben oder Optimierungsvorschläge. Die Auswertung der Daten und die Planung und Optimierung der System Sicherheit liegt in der Verantwortung des Sicherheitsverantwortlichen.

Das Sammeln der Informationen muss explizit gestartet werden und erfolgt nicht automatisch. Die Auswertung der gesammelten Daten erfolgt über den IBM Navigator for i oder über individuelle SQL Abfragen.

Aktivierung und Beendigung einer Authority Collection

Das Erfassen der Zugriffsdaten erfolgt immer für ein Benutzerprofil. Bei dem Befehl STRAUTCOL muss ich ein Benutzerprofil angeben dessen Zugriffsdaten ich erfassen möchte. Für jedes Benutzerprofil dessen Daten gesammelt werden sollen, muss ich einen STRAUTCOL Befehl absetzen. Es ist wichtig, das effektive Benutzerprofil auszuwählen unter dem der Job ausgeführt wird. Ich kann bei STRAUTCOL auch ein Gruppenprofil angeben, dann werden aber keine Daten erfasst außer das Gruppenprofil ist der effektive Benutzer eines Jobs.

Das gilt auch für den Eigner eines Objektes. Als kleines Beispiel folgende Überlegung.
OWN1 ist der Eigner des Programms PGM1 und dieses Programm verwendet Adopted Authority. Es verwendet also die Berechtigungen von OWN1. Wenn der Benutzer USR1 dieses Programm benutzt, ich bei STRAUTCOL aber den Benutzer OWN1 angebe, dann werden keine Zugriffsdaten für die Verwendung dieses Programms aufgezeichnet. Ich muss die Authority Collection für den Benutzer USR1 starten, um zu sehen auf welche Objekte der Benutzer USR1 zugegriffen hat. In den aufgezeichneten Daten sieht man dann, dass das Programm PGM1 Adopted Authorities vom Benutzer OWN1 verwendet.

Beim Aufrufen von STRAUTCOL kann ich umfangreiche Angaben zu den Objekten machen, für die ich Zugriffsdaten aufzeichnen möchte. Als Standard werden alle Objekte und alle Objekt Typen (z. B. *FILE, *PGM ..) im System ASP aufgezeichnet.
Ich kann nur bestimmte Objekt Typen auswählen, mit Wildcards den Namen der Objekte einschränken oder nur Objekte in einer ausgewählten Bibliothek aufzeichnen.
Auch Zugriffe auf IFS und DLO Objekte können aufgezeichnet werden und es ist auch möglich einen User ASP auszuwählen.

Um vollständige Daten zu erhalten, ist es wichtig die Aufzeichnung bis zur Beendigung der Anwendung inklusive dem Full Close der Dateien durchzuführen. Nur dadurch ist sichergestellt, dass alle relevanten Zugriffsinformationen erfasst werden.

Beendet wird eine aktive Authority Collection mit dem Befehl ENDAUTCOL. Auch bei diesem Befehl muss ein Benutzerprofil angegeben werden. Der Befehl ENDAUTCOL USRPRF(WGTEST) beendet das Sammeln von Zugriffsdaten für den Benutzer WGTEST.

Löschen von gesammelten Zugriffsdaten
Zugriffsdaten die nicht länger benötigt werden, lassen sich mit dem Befehl DLTAUTCOL löschen. Das Löschen der Daten erfolgt immer für ein Benutzerprofil. Um die Daten für das Benutzerprofil WGTEST zu löschen verwenden wir den Befehl

```
DLTAUTCOL USRPRF(WGTEST)
```

Das regelmäßige Löschen von Daten in einer Authority Collection ist sinnvoll, um einen übersichtlichen Datenbestand zu erhalten. Eine Authority Collection kann nur gelöscht werden wenn sie nicht aktiv ist.

Weiterführende Informationen

Umfangreiche Informationen zum Thema Authority Collections finden Sie im IBM Knowledge Center: https://ibm.biz/Bdjy8Z
Weiterführende Informationen zum Thema Security für IBM i 7.3 finden Sie hier: https://ibm.biz/BdjyU6

IBM i 7.3 Informationen im IBM Knowledge Center: https://ibm.biz/Bd4V8C
Eine aktuelle IBM i Roadmap und weitere Informationen finden Sie hier: https://ibm.biz/Bdsv7V

Über den Autor

Der Autor Willy Günther ist Senior IT Spezialist bei der IBM Deutschland GmbH
wiguenth (ät) de.ibm.com