Produktbeschreibung

opusR RACF-data warehouse

Auf einen Blick

opusR ist ein data warehouse aller sicherheitsrelevanten Informationen um RACF.

Die Daten werden aus vorhandenen Quellen gewonnen oder durch Monitoring erzeugt.

Analysetool und Batch-Ausgabe auf verschiedene Plattformen inkludiert.

Kein Schulungsaufwand, keine eigene Sprache.

Seit 10 Jahren am Markt, sehr gutes Preis-Leistungsverhältnis.

Key Features

24x7 *volles* RACF-Monitoring

Data warehouse über wesentliche RACF-Datenquellen mit Datenkonsistenz untereinander verknüpft

Speicherung ALLER Zugriffe Langzeit durch Verdichtungsmöglichkeit

Data cube Analysearchitektur

Komplexe Analysen als Zeilenbefehl

Hunderte Reports generierbar

opusR ist Monitoring, Datensammlung und Analyse

opusR sammelt für Sicherheitsüberprüfungen nötige Daten aus verschiedenen, heterogenen Quellen und bringt sie in eine normierte, konsistente Form. Die Auswertung dieses data warehouse erfolgt mit Standard-SQL wobei viele, teils komplexe Abfragen als einfache Display-Befehle eingebaut sind. Ausgabe und Weiterverarbeitung auf z/OS und Client-Plattformen sind inkludiert. Die Datenhaltung ist systemübergreifend und kann auf einem System, das nicht das Überwachte ist, erfolgen.

opusR data warehouse

Die Sammlung der Daten erfolgt aus sehr heterogenen Quellen. Diese Daten werden durch opusR in eine normierte, mit relationalen Mitteln auswertbare Form gebracht.

RACF-Datenbank

Die RACF-Datenbank wird mit allen Informationen aus dem FLATFILE übernommen.

Informationen aus Kontrollblöcken

Aus verschiedenen Kontrollblöcken werden sicherheitsrelevante Informationen gesammelt. (APF-Libraries, LINKLIST et. al.)

RACF-Commands

Alle ausgeführten RACF-Befehle werden direkt aus dem RACF-Command-Exit aufgezeichnet und in eine Beziehung zur RACF-Datenbank gesetzt.

Zugriffsdaten

Alle Zugriffe auf Ressourcen werden von opusR an den RACF-Exits aufgezeichnet. Unser größter Kunde hat mehr als 2.000.000.000 Zugriffe pro Tag, in der Spitze haben wir 120.000 Zugriffe pro Sekunde gemessen.
Diese Daten werden in eine Relation zur RACF-Datenbank gesetzt.
(Zur Erläuterung: Die Ressource SYS1.PARMLIB wird vom Profil SYS1.** geschützt)
Da sich die RACF-Datenbank ständig ändert, werden auch diese Beziehungen aktualisiert um die Relation konsistent zu halten.

Beispiel

Frage:

Welche Permits einer Gruppe sind wie benutzt?

Antwort:

- Suche User in der Gruppe und deren benutzte Ressourcen im CONNECT-Zeitraum

- Suche Profile die durch die Gruppe ermächtigt sind

- Bringe Profile und Ressourcen zusammen und ermittle das höchste Zugriffsdatum.

Technische Voraussetzungen

z/OS 2.1 oder höher

RACF ab 1.1.9

DB2 11.0 oder höher

opusR Auswertungen

Die data cube-Architektur der opusR Daten ermöglicht durch unser Display den Einstieg über 6 Ebenen und lässt Analysen in jede Richtung zu.

Der Dialog ist einfach und intuitiv. Eine Auswertungssprache brauchen Sie nicht zu lernen.

Aus jedem Selektionsergebnis kann endlos in neue Selektionen verzweigt werden. Zur schnellen Übersicht kann jedes Ergebnis gruppiert werden. Tiefenanalysen sind schnell durchführbar. Einzelne Zeilenbefehle führen oft komplexe Analysen aus. Ein Beispiel finden sie im Kasten links.

Aus jeder Auswertung kann mit einem einfachen Tastendruck eine Batch-Auswertung generiert werden. Die Ausgabe der Daten auf Datei, USS-Path (Netzlaufwerk) oder Mail ist vorgesehen.

Diese Auswertungen sind Basis für Bereinigungen, Revisionen, Audits und Reports. Aus der Dialoganzeige können mit einem Befehl Commands generiert werden, die eine beliebige Weiterverarbeitung ermöglichen.

opusR und Identity-Management

Moderne Benutzerverwaltungen über IAM (Identity Access Management)-Systeme vergeben und entziehen den Benutzern Rechte. Der Rechteentzug beim Wechsel einer Tätigkeit ist eine geforderte Voraussetzung von externen Revisionsstellen.

opusR erstellt in einfachen Dialogschritten Rollen nach Minimalprinzip für beliebige IAM-Systeme, erlaubt deren Revision in Dialog und Batch. Bestehende Gruppen werden mit einbezogen.