RACFBroker/j

Entfernter Zugriff auf das
RACF Sicherheitssystem
auf IBM Mainframes
über TCP/IP

RACFBroker/j ist ein Produkt der

XPS Software GmbH
Eching

RACFBroker/j

XPS Software GmbH
Untere Hauptstr. 2
85386 Eching

Tel.: +49 (0)89-456989-0
Fax: +49 (0)89-456989-29
Web: http://www.xps-software.de
E-Mail: info@xps-software.de

Copyright

Warenzeichen

Einleitung

Dieses Dokument beschreibt die Nutzung der Software RACFBroker/j, einem Produkt der XPS Software GmbH, Eching.

RACFBroker/j ist eine Java Programmierschnittstelle, die Anwendungsprogrammen in heterogenen Netzwerken eine Schnittstelle zur Nutzung ausgewählter Funktionen der IBM Mainframe Sicherheitssysteme RACF (Resource Access Control Facility), ACF/2 und TopSecret zur Verfügung stellt. RACFBroker/j basiert auf dem Produkt TRex von XPS.

RACFBroker/j kann ausschließlich im Zusammenspiel mit RACFBroker/z eingesetzt werden. RACFBroker/z ist ein IBM Mainframeprogramm, das die benötigten Zugriffe auf das Mainframe Sicherheitssystem zur Verfügung stellt. RACFBroker/z basiert auf dem Produkt XPSDaemon von XPS und ist in Gegenstand einer eigenen Beschreibung.

Das nachfolgende Schaubild zeigt das konzeptuelle Zusammenspiel der beteiligten Komponenten:

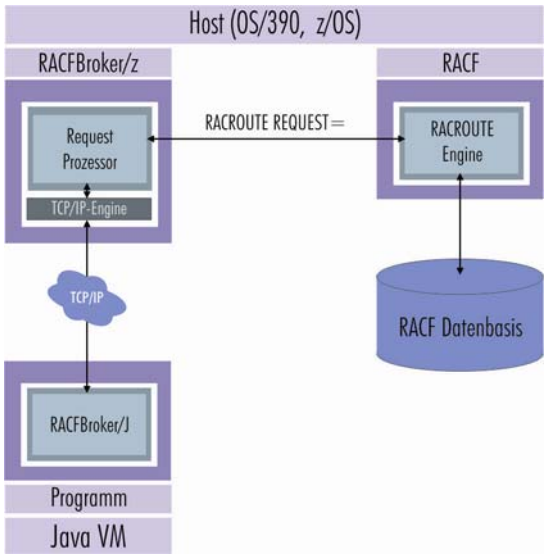

Abb. 1: RACFBroker-Konzept

Ein Java bzw. ein Win32 Programm stellt unter Verwendung des RACFBroker/J APIs eine RACF Anfrage an RACFBroker/z.

Dazu wird zwischen beiden Rechnern eine geschützte TCP/IP Verbindung aufgebaut. Pro Session wird ein symmetrischer Schlüssel erzeugt, der unter Verwendung eines RSA public/private Schlüsselpaares zwischen RACFBroker/z und RACFBroker/J ausgetauscht wird.

Der gesamte Datenaustausch wird dann unter Verwendung des symmetrischen Schlüssels wahlweise mit AES (Advanced Encryption Standard – Rijndael), Triple DES oder Blowfish verschlüsselt abgewickelt, um die Integrität der übertragenen Daten sicherzustellen.

RACFBroker/z leitet die Anfrage unter Verwendung der RACF Programmierschnittstelle RACROUTE an die entsprechende Engine weiter, die diese unter Zugriff auf die RACF Datenbasis ausführt.

Das Ergebnis der Ausführung der Anfrage wird dann von RACFBroker/z an RACFBroker/J zurückgemeldet und dem Anwendungsprogramm zur Auswertung zur Verfügung gestellt.

Inhalt des Programmpaketes

RACFBroker/j wird als komprimiertes Archiv 'racfbrokerj.zip' ausgeliefert. Das Archiv hat die nachfolgend abgebildete Struktur:

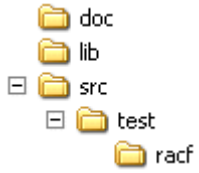

Abb. 2: RACFBRoker/j - Programmpaket

Das Verzeichnis 'doc' enthält die Beschreibung der RACFBroker/j Programmierschnittstelle im Javadoc Format.

Das Verzeichnis 'lib' enthält das signierte Programmarchiv 'jbroker.jar', das alle benötigten Klassendateien sowie die zu Grunde liegenden Klassenbibliotheken zur Nutzung der Programmierschnittstelle enthält.

Darüber hinaus enthält 'jbroker.jar' das Programm 'RACFBrokerTester', mit dessen Hilfe sämtliche Funktionen von RACFBroker/j unter Verwendung einer graphischen Benutzeroberfläche getestet werden können.

Das Verzeichnis 'src' enthält den Java Quellcode für das RACFBroker Testprogramm 'RACFBrokerTester.java'. Der Quellcode kann ohne Einschränkungen in eigene Anwendungen integriert und verändert werden.

Vorgehensweise zur Nutzung von RACFBroker/j

Die nachfolgende Auflistung enthält die notwendigen Schritte, die ein Anwendungsprogramm durchführen muss, um die RACFBroker Funktionalität nutzen zu können. Angaben in eckigen Klammern '[]' beziehen sich auf Funktionen der RACFBroker/j Programmierschnittstelle.

1. Erstellen einer 'RACFBroker' Instanz, der unter anderem die benötigten Daten zum Aufbau einer Verbindung mit der Hostkomponente RACFBroker/z zu übergeben sind [new RACFBroker()].
2. Nutzung der erstellten RACFBroker Instanz zum Aufbau einer Verbindung mit dem gewünschten RACFBroker/z Hostprogramm [RACFBroker.establishConnetion()].
3. Erstellen einer 'RACFBrokerRequest' Instanz mit der in nachfolgenden Schritten Anfragen durchgeführt werden (new RACFBrokerRequest()].
4. Füllen der 'RACFBrokerRequest' Instanz mit anfragespezifischen Daten (RACFBrokerRequest.setXXX()].
5. Übermitteln der Anfrage an RACFBroker/z [RACFBroker.executeRequest(...)].
6. Auswerten der Rückgabewerte (RACFBrokerRequest.getXXXReturnCode()].
7. Wiederholen der Schritte 4. bis 6. (optional).
8. Beenden der Verbindung mit RACFBroker/z [RACFBroker.terminateConnection()].

Das RACFBroker Testprogramm

Zur Veranschaulichung der Nutzung der RACFBroker/j Programmierschnittstelle ist ein Testprogramm samt Java Quellcode Bestandteil des RACFBroker/j Programmpaketes.

Das Testprogramm kann auf Plattformen, die den Mechanismus der 'executable jars' unterstützen, durch Doppelklick bzw. durch den Aufruf

```
'java –jar jbroker.jar'
```

gestartet werden. Sollte dies nicht funktionieren, ist der alternative Aufruf

```
'java –cp jbroker.jar test.racf.RACFBrokerTester'
```

möglich.

Die verschiedenen Eingabemasken

Das RACFBroker Testprogramm erlaubt die Eingabe der relevanten Daten für jede mögliche RACF Anfrage in einer eigenen Dialogseite.

Überprüfung eines Passwortes auf Gültigkeit

Mit der nachfolgend abgebildeten Maske kann das Passwort eines RACF Benutzers auf Gültigkeit geprüft werden:

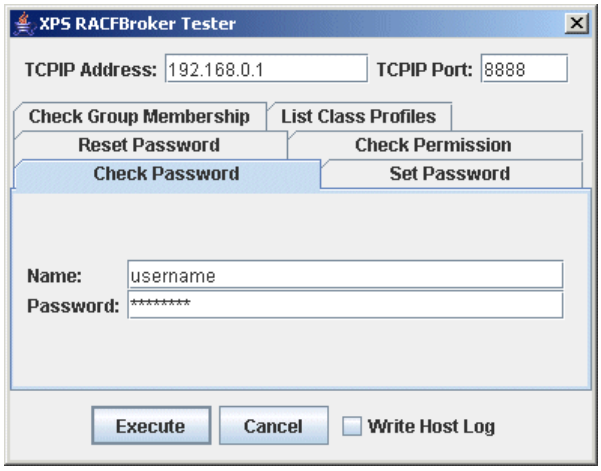

Abb. 3: Testprogramm – Check Password

Im oberen und unteren Bereich des Dialogs befinden sich Kontrollen, die für alle Funktionen verfügbar sind:

TCPIP Address	Angabe der TCP/IP Adresse des Hostrechners, auf dem RACFBroker/z installiert ist.
TCPIP Port	Angabe des TCP/IP Ports, der von RACFBroker/z überwacht wird.
Execute	Die momentan angezeigte RACFBroker Funktion wird ausgeführt.
Cancel	Das Testprogramm wird beendet.
Write Host Log	Selektieren dieser Checkbox bewirkt, dass RACFBroker/z einen Eintrag für die ausgeführte Funktion in sein Joblog schreibt. Dieses Log kann

von einem Systemprogrammierer zur Auswertung der ausgeführten RACF Funktionen herangezogen werden.

Der zentrale Bereich des Dialogs beherbergt jeweils die Kontrollfelder, die zur Ausführung der angezeigten Funktion notwendig sind.

Name In diesem Feld ist der Name des RACF Benutzers anzugeben, für den die Überprüfung des Passwortes durchgeführt werden soll.

Password In diesem Feld ist das Passwort anzugeben, das auf Gültigkeit überprüft werden soll. Im diesem, wie in allen anderen Passwort Eingabefeldern auch, erscheint pro eingegebenem Zeichen das Ersatzzeichen '*'. D. h., dass das Passwort nicht lesbar ist.

Durch Drücken der Schaltfläche 'Execute' wird die Ausführung der jeweils aktiven Anfrage - hier die Überprüfung der eingegebenen Name/Passwort Kombination - veranlasst.

Vergeben eines neuen Passwortes

Mit der nachfolgend abgebildeten Maske kann für einen RACF Benutzer ein neues Passwort vergeben werden:

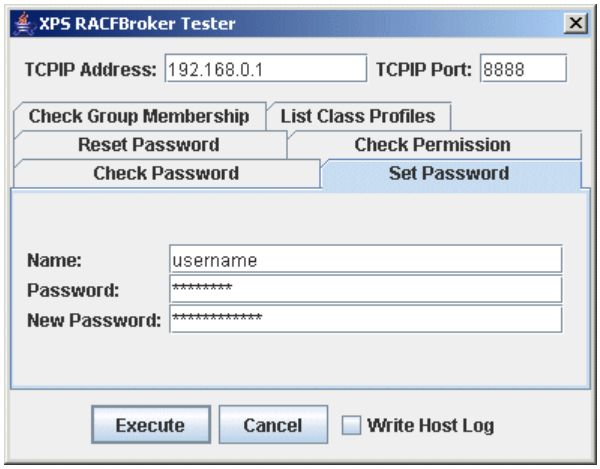

Abb. 4: Testprogramm – Set Password

Name In diesem Feld ist der Name des RACF Benutzers anzugeben, für den das Passwort neu gesetzt werden soll.

Password In diesem Feld ist das aktuelle Passwort für den Benutzer anzugeben.

New Password In diesem Feld ist das neue Passwort für den Benutzer anzugeben.

Zurücksetzen eines Passwortes

Mit der nachfolgend abgebildeten Maske kann für einen RACF Benutzer das Passwort zurückgesetzt werden:

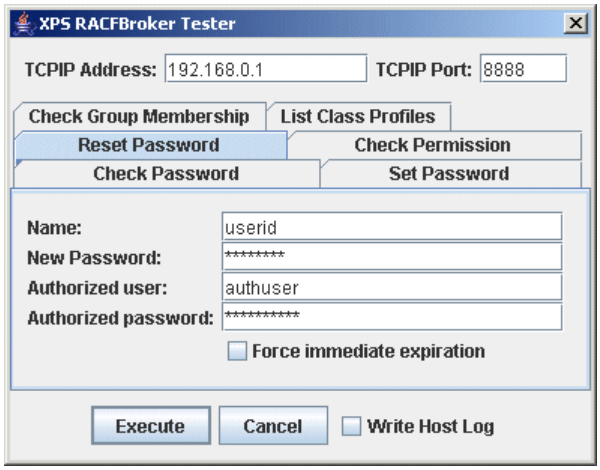

Abb. 5: Testprogramm – Reset Password

Name In diesem Feld ist der Name des RACF Benutzers anzugeben, für den das Passwort zurückgesetzt werden soll.

New Password In diesem Feld ist das neue Passwort für den Benutzer anzugeben.

Authorized User In diesem Feld ist der RACF Name eines Benutzers anzugeben, der zur Ausführung der Reset Funktion berechtigt ist. Die Passwort Reset Funktion beinhaltet ein kritisches sicherheitsrelevantes Potenzial, da zum Rücksetzen des Passworts das aktuell gültige Passwort **nicht** bekannt sein muss. Beim Starten der Hostkomponente RACFBroker/z ist festzulegen, ob ein Benutzer über das RACF Attribut 'Special' verfügen muss, um diese Funktion auszuführen. Es wird dringend empfohlen, diese standardmäßige Einschränkung nicht aufzuheben.

Authorized password In diesem Feld ist das aktuell gültige Passwort für den zur Funktionsausführung autorisierten Benutzer anzugeben. RACFBroker/z bearbeitet die Anfrage nur dann, wenn der autorisierte Benutzer im RACF mit dem geforderten Attribut 'Special' definiert ist, und das angegebene Passwort für den autorisierten Benutzer aktuell gültig ist.

Force immediate expiration Durch Auswahl dieser Checkbox wird erreicht, dass das im Rahmen des Reset neu vergebene Passwort für den Benutzer sofort als nicht länger gültig gekennzeichnet wird. Dies hat zur Folge, dass der Benutzer bei der nächsten Anmeldung an das Hostsystem zur Vergabe eines neuen Passworts aufgefordert wird.

Überprüfen der Zugriffsbefugnis eines Benutzers

Mit der nachfolgend abgebildeten Maske kann festgestellt werden, ob ein Anwender eine bestimmte Zugriffsberechtigung für eine RACF Ressource besitzt:

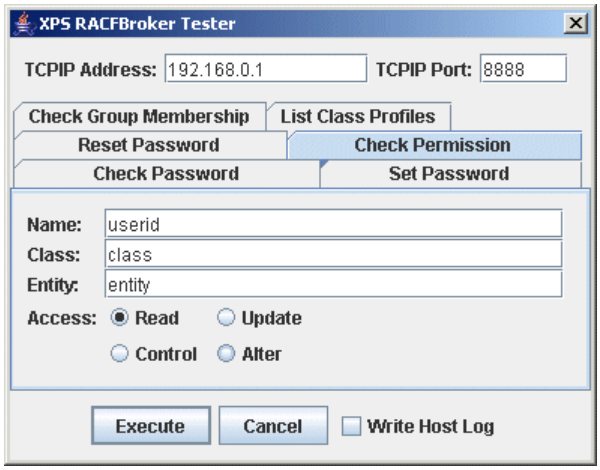

Abb. 6: Testprogramm – Check permission

Name In diesem Feld ist der Name des RACF Benutzers anzugeben, für den die Überprüfung durchgeführt werden soll.

Class In diesem Feld ist der Name der RACF Klasse anzugeben, in der die zu überprüfende Ressource definiert ist.

Entity In diesem Feld ist der Name der Ressource anzugeben, für die die Überprüfung durchgeführt werden soll.

Access Mit dieser Gruppe von Radio Kontrollen ist festzulegen, welcher Level von Zugriffsrecht des Benutzers für die angegebene Ressource geprüft werden soll. Die möglichen Optionen entsprechen den originalen Bezeichnungen im RACF.

Überprüfen der Gruppenzugehörigkeit eines Benutzers

Mit der nachfolgend abgebildeten Maske kann festgestellt werden, ob ein Benutzer Mitglied in einer bestimmten RACF Gruppe ist:

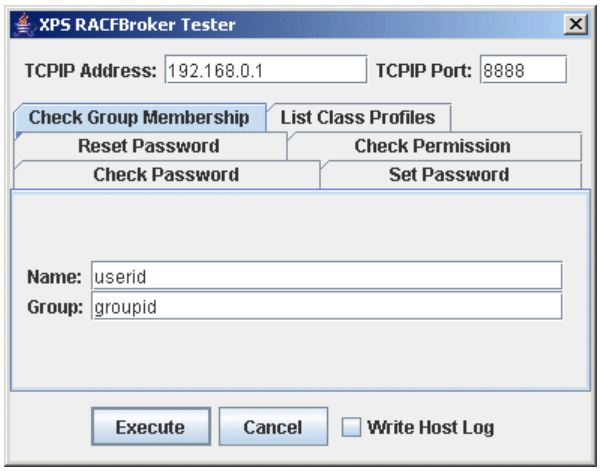

Abb. 7: Testprogramm – Check Group Membership

Name In diesem Feld ist der Name des RACF Benutzers anzugeben, für den die Überprüfung durchgeführt werden soll.

Group In diesem Feld ist der Name der RACF Gruppe anzugeben, für die die Mitgliedschaft des Benutzers geprüft werden soll.

Auflisten der Profile in einer RACF Klasse

Mit der nachfolgend abgebildeten Maske kann eine Liste der Profile, die in einer RACF Klasse definiert sind, erstellt werden:

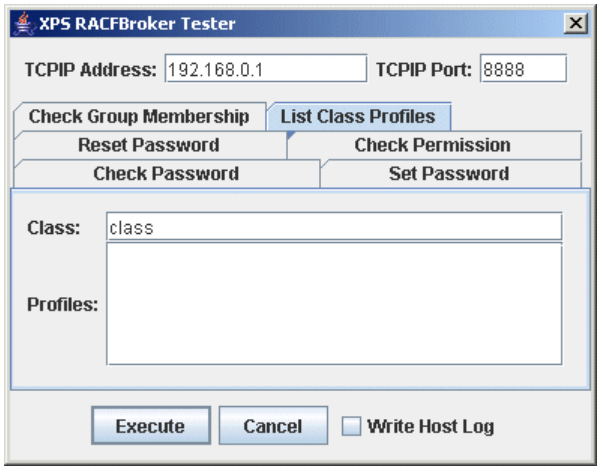

Abb. 8: Testprogramm – List Class Profiles

Class In diesem Feld ist der Name der RACF Klasse anzugeben, für die die enthaltenen Profile ermittelt werden sollen.

Profiles In diesem Feld wird das Ergebnis der Abfrage angezeigt.