

[← Zum Hauptmenü](#)

Übersicht Rollenrechte

Die per RSBAC erstellten Rollen beinhalten eine Reihe von Rechten, welche die Zugriffe der ausgeführten Programme auf andere Ressourcen (wie Dateien, Netzwerk-Ports und Devices) beschränken oder ermöglichen.

Hintergrund: In einem Linux Betriebssystem mit RSBAC-Erweiterung können neben dem Linux-immanenten Zugriffsrechte-Modell noch weitere Zugriffsrechte-Modelle geladen und die Rechte miteinander kombiniert werden. Dabei verstehen wir unter Rechten auch Beschränkungen. Bei allen Servern der m-privacy GmbH haben wir uns insbesondere für das Role Compatibility (RC)-Modell entschieden. Das RC-Modell erlaubt eine wesentlich feinere Rechtevergabe als das Standard-Zugriffsrechte-Modell unter Linux. Die einzelnen Rollen beschreiben jeweils ein Subset an Regeln, welches für die jeweilige Rolle bedeutsam ist.

Die Rolle CONFIG

Die Rolle CONFIG ist für den speziellen Benutzeraccount *config* vorgesehen, welcher die Aufgabe hat, die spezifischen (Netzwerk-)Anpassungen für die mp-Firewall an das lokale Netz vorzunehmen. Die wichtigsten mit dieser Rolle verbundenen Rechte sind in den folgenden Tabellen aufgeführt:

+/-	Rolle CONFIG
+	Auf Menüfunktionalität beschränktes Ändern von Netzwerkeinstellungen.
+	Neustart des Systems.
-	Individuelles Ändern von Konfigurationsdateien
-	Vergabe von Zugriffsrechten
-	Shell-Zugriff
-	Grafische Oberfläche

Die Rolle MAINT

Die Rolle MAINT wird vom lokalen Benutzer-Administrator *maint* zur Nutzerverwaltung verwendet und ermöglicht das Anlegen und Löschen von Benutzern sowie die Vergabe von (initialen) Passwörtern. Die wichtigsten mit dieser Rolle verbundenen Rechte sind in den folgenden Tabellen aufgeführt:

+/-	Rolle MAINT
+	Auf Menüfunktionalität beschränkte Benutzerverwaltung
+	Neustart des Systems und einzelner Komponenten
+	Zeitbeschränkte Zulassung von Administrator-Anmeldungen per SSH über Netzwerk zur Systemwartung
+	Zulassung von Anmeldungen per SSH über Netzwerk von außerhalb des vorgesehenen Klientennetzwerkes
-	Individuelles Ändern von Konfigurationsdateien

+/-	Rolle MAINT
-	Vergabe von Zugriffsrechten
-	Shell-Zugriff
-	Grafische Oberfläche

Die Rolle SECURITY

Die Rolle SECURITY bestimmt die Möglichkeiten des Sicherheitsbeauftragten (auch SecOff genannt). Diese Rolle kann das gesamte RSBAC-Regelwerk bearbeiten: Es können neue Rollen definiert und Rechte bestehender Rollen geändert werden. Wegen seiner Mächtigkeit ist die Rolle SECURITY in der Voreinstellung nur von der lokalen Konsole aus zugänglich. Ein SSH-Remote-Zugang für SECURITY kann nur durch MAINT für einen begrenzten Zeitraum aktiviert werden. Eine Übersicht über die Besonderheiten der Rolle SECURITY zeigt die Tabelle:

+/-	Rolle SECURITY	Bemerkung
+	Editieren sämtlicher RSBAC-Regeln	
+	Prüfen aller Protokolldateien	
+	Nur-Lese-Zugriff auf Benutzerdaten	
-	Grafische Oberfläche	
-	Netzwerkzugriff	(ohne weitere Rechtevergabe)

Die Rolle ROOT

Die Rolle ROOT entspricht im wesentlichen dem klassischen Systemverwalter für Systemdienste. Als ROOT können installierte Systemdienste gestartet und angehalten werden, es können Tests mit Systemwerkzeugen durchgeführt und eingeschränkt Systemdienste konfiguriert werden. Gegenüber dem allmächtigen root-Account eines normalen Linux-Systems unterliegt die Rolle ROOT besonderen Beschränkungen. So kann ROOT insbesondere nicht auf die Verzeichnisse der Benutzer zugreifen, kann keine Programme mit RSBAC-Rechten ausstatten und generell keine RSBAC-Rechte ändern, wohl aber die RSBAC-Rechte ansehen. Eine Übersicht über die Besonderheiten der Rolle ROOT zeigt die Tabelle:

+/-	Rolle ROOT	Bemerkung
+	Editieren der Konfiguration von ungeschützten Systemdiensten	
+	Nutzung von Test-Tools	(z.B. netstat)
+	Installation von Programm-Paketen außerhalb der Standard-Pfade	Zur Ausführung notwendige RSBAC-Rechte müssen von SECURITY vergeben werden!
+	Aufruf von „rsbac_menu“ nur lesend	
-	Zugriff auf /home-Verzeichnisse	
-	Editieren von geschützten Konfigurationsdateien	
-	Grafische Oberfläche	

Die Rolle UPDATE

Die Rolle UPDATE dient der unkomplizierten Aktualisierung von Servern. UPDATE vereinigt die Möglichkeiten des Netzwerkzugriffs (z.B. mittels ssh) und des Updates von Programm-Paketen mittels

eines Paketmanagers. Eine Übersicht über die Besonderheiten der Rolle UPDATE zeigt die Tabelle:

+/-	Rolle UPDATE	Bemerkung
+	Starten von Paket-Updates	
+	Sichern und Zurückspielen der RSBAC-Konfiguration da bei der Aktualisierung Attribute gelöscht werden können.	
+	Über Menüfunktionalität beschränkte Aktualisierung der installierten Programmpakete	Zur Ausführung notwendige RSBAC-Rechte müssen von SECURITY gesetzt werden!
-	Grafische Oberfläche	
-	Zugriff auf /home-Verzeichnisse	
-	RSBAC-Konfiguration ändern	
-	Shell-Zugriff	

Die Rolle BACKUSER

Die Rolle BACKUSER dient der Erstellung von Backups und zum Rücksicherung von bestehenden Backups. BACKUSER hat als einzige Rolle die Möglichkeit für die Erstellung von Backups auf /home-Verzeichnisse zuzugreifen. Es ist BACKUSER nicht erlaubt Programme zu installieren oder eine Inhaltskontrolle der /home-Verzeichnisse vorzunehmen. Eine Übersicht über die Besonderheiten der Rolle BACKUSER zeigt die Tabelle:

+/-	Rolle BACKUSER	Bemerkung
+	Lese/Schreibe-Zugriff auf das CD/DVD und das Bandlaufwerk	Beschränkt auf das Sichern/Rücksichern von Backups
+	Netzwerkzugriff	Beschränkt auf Backup-Server
+	Lese/Schreib-Zugriff auf /home-Verzeichnisse	Keine Inhaltskontrolle möglich!
+	Über Menüfunktionalität Erstellung neuer und Rücksicherung bestehender Backups	
-	Grafische Oberfläche	
-	RSBAC-Konfiguration ändern	
-	Shell-Zugriff	

< Zum Hauptmenü

From:

<https://help.m-privacy.de/> -

Permanent link:

<https://help.m-privacy.de/doku.php/tightgate-firewall:rollenrechte>

Last update: **2020/09/25 07:58**

