

# NetScaler Ressourcenzuweisung an Gruppen – Teil I

Hallo zusammen

Immer wieder wird im Zusammenhang mit NetScaler die Frage gestellt: „Kann ich Ressourcen auch Gruppen zuweisen?“

Die Antwort ist kurz und bündig „Ja, man kann“, aber das wie und wo, das will ich in mehreren Artikeln ein wenig erläutern. In diesem ersten will ich auf das wohl häufigste Szenario, dem NetScaler Gateway eingehen.

Auf die Einschränkung bei der Anmeldung möchte ich hier jedoch nicht eingehen. Dies ist in [CTX111079](#) schon ausführlich beschrieben.

Viele kennen den NetScaler Gateway so, dass sie die virtuellen Server mittels Wizard aufsetzen, testen und für gut befinden. Daran gibt es kaum was auszusetzen. Wenn jedoch die Anforderungen wachsen und die Ressourcen (Session Policies) gemäss AD Gruppenmitgliedschaft zugewiesen werden sollen, dann funktioniert dies nicht mehr so sauber.

Das NetScaler System bietet uns hierzu ein paar gute Möglichkeiten. Bevor ich detaillierter auf so eine Konfiguration eingehe, möchte ich aber noch ein paar Worte zu den „Bind Points“ und Prioritäten verlieren.

## **Bind Points**

Es gibt bei NetScaler Gateway vier Orte, wo wir die Session Policies binden können:

Benutzer -> Gruppen -> virtueller Server -> Global

*Global:*

Die globalen Einstellung sind zwar keine Session Policy, jedoch beinhalten sie die gleichen Einstellungen. Die globalen

Einstellungen sind in der Hierarchie ganz unten und kommen somit erst zum Zug, wenn keine Session Policy was anderes definiert.

#### *virtueller Server:*

Beim der Zuweisung der Session Policies an einen virtuellen Server schränken wir dessen Aktionsradius auf diesen einen vServer ein. Dieser „Bind Point“ ist einer Hierarchie-Stufe höher wie die globalen Einstellungen.

#### *Gruppen:*

Es können Gruppen angelegt werden. Diese müssen exakt so wie in der AD geschrieben sein (case-sensitive). Diesen können Session Policies zugewiesen werden, welche dann nur für Mitglieder dieser Gruppe gelten. Die Gruppen haben die zweithöchste Hierarchie-Stufe.

#### *Benutzer:*

Es können auch Benutzer angelegt werden, welche wie die Gruppen mit der AD überein stimmen müssen. Diese haben die höchste Hierarchie-Stufe, sollten jedoch zur vereinfachten Administration höchstens zu Testzwecken benutzt werden.

## **Prioritäten**

Wenn eine Policy zugewiesen wird, wird immer eine Priorität vergeben. Je kleiner die Nummer, desto höher die Priorität.

Gemeinerweise übersteuert die Priorität die soeben beschriebene Hierarchie der „Bind Points“, d.h. eine Policy gebunden an den vServer mit Prio 10 hat Vorrang einer Policy gebunden an eine Gruppe mit Prio 100.

Um dem Vorzubeugen habe ich mir persönlich angewöhnt mit Prioritätsbereichen zu arbeiten:

vServer: in Hunderterschritten 100, 200, 300, etc.

Gruppen: in Zehnerschritten: 10,20,30, etc.

Benutzer: in Einerschritten: 1,2,3, etc.

So sollte man sich selbst kein Bein stellen.

# Beispielskonfiguration NetScaler Gateway

Im folgenden Beispiel will ich zwei verschiedene Session Policies (Apps Only / VPN) zwei verschiedenen Gruppen zuweisen. Ich gehe dabei davon aus, dass die Session Policies bereits erstellt sind und fokussiere mich nur um die Zuweisung auf die verschiedenen Gruppen.

Als erstes müssen die zwei Gruppen erstellt werden:

```
add aaa group G_PIT_AppsOnly
add aaa group G_PIT_VPNOnly
```

Anschliessend werden die vom Wizard erstellten Policies vom vServer entfernt:

```
unbind vpn vserver nsgw-vsrv-gateway.domain.pit -policy
Policy01
unbind vpn vserver nsgw-vsrv-gateway.domain.pit -policy
Policy02
```

Um im dritten Schritt die entsprechenden Policies den Gruppen zuzuweisen:

```
bind aaa group G_PIT_AppsOnly -policy SESPOL-AppsOnly
bind aaa group G_PIT_VPNOnly -policy SESPOL-VPNOnly
```

Viel Spass beim nachbauen :-)

Skript: [NS-ResToGroup1](#)