ACL-Syntax (Login-Knoten)

Verwendung des Storage-Knotens für ACLs

Der Login-Knoten greift nur über einen NFS-Export auf das GPFS zu, anstelle wie die Rechenknoten und Storage-Knoten nativen Zugriff zu haben. Daher ist die Steuerung der ACLs vom Login-Knoten aus nur eingeschränkt möglich. Es wird daher empfohlen, die Verwaltung der ACLs direkt über den Storage-Knoten vorzunehmen.

Syntax (Login-Knoten)

Die ACLs bestehen aus mehreren Einträgen, welche jeweils die Berechtigungen für einen Nutzer oder eine Nutzergruppe spezifizieren. Zusätzlich zu den Berechtigungen kann die Funktionsweise der ACLs durch einen Typ oder verschiedene Flags beeinflusst werden. Die vollständige Syntax für das auf dem Login-Knoten verwendete `nfs4_setfacl` lautet:

nfs4_setfacl syntax

```
type:flags:principal:permissions
```

Typ

Es gibt vier verschiedene Typen an ACL-Einträgen, die die Bedeutung der Berechtigungen regeln:

Typ	Bedeutung	Beschreibung
A	Erlauben (Allow)	Erlaube dem Nutzer die gegebenen Berechtigungen
D	Verweigern (Deny)	Verweigere dem Nutzer die gegebenen Berechtigungen
U	Protokollieren (Audit)	Protokolliere Zugriffe des Nutzers auf die gegebenen Berechtigungen
L	Alarmieren	Erzeuge einen Systemweiten Alarm beim Zugriff des Nutzers auf die gegebenen Berechtigungen

Für uns sind nur die ersten beiden Typen relevant.

Flags

Flags steuern z.B. die Weitergabe / Vererbung der ACLs an Unterordner / Dateien, oder erlauben es, eine Nutzergruppe statt einem einzelnen Nutzer zu spezifizieren

Flag	Bedeutung	Beschreibung
g	Gruppe	Der angegebene "Principal" ist eine Gruppe, kein Nutzer
d	Verzeichnis-Vererbung	Vererbe die Berechtigungen an neue Unterverzeichnisse
f	Dateivererbung	Vererbe die Berechtigungen an neue Dateien
n	Einzelvererbung	Vererbe die Berechtigungen nur an Unterverzeichnisse der 1. Ebene
i	Nur Vererbung	Die Berechtigungen gelten nur für neue Unterverzeichnisse / Dateien (entsprechend `d` oder `f`) und nicht für das aktuelle Verzeichnis

Zielnutzer / -gruppe

"Principal" ist der Nutzer (oder die Gruppe bei Verwendung von Flag `g`) für den die Berechtigungen gelten. Es gibt zusätzlich drei Sondertypen: `OWNER@`, `GROUP@` und `EVERYONE@`, die den POSIX-Berechtigungen Besitzer / Gruppe / Andere entsprechen.

Berechtigungen

Berechtigungen steuern die tatsächlichen Berechtigungen des jeweiligen ACL-Eintrags.

Berechtigung	Bedeutung für Dateien	Bedeutung für Ordner
r	Dateien lesen	Ordnerinhalte auflisten
w	Dateien schreiben	Neue Dateien anlegen
a	Daten an Datei anhängen	Unterordner anlegen
x	Dateien ausführen	Ordner öffnen
d	Datei löschen	Ordner löschen
D	-	Datei oder Unterordner im Ordner löschen
t	Attribute lesen	
T	Attribute schreiben	
n	"Named Attributes" lesen	
N	"Named Attributes" schreiben	
c	NFSv4-ACL lesen	
C	NFSv4-ACL schreiben	
o	Dateieigentümer und Gruppe ändern	
y	Synchronisierten Datenverkehr anfordern	

Ein paar Beispiele

Recht	NFSv4 ACL-Flags
Nur Ordner öffnen (benötigt für den Zugriff auf Unterordner)	xc
Nur Lesen	rtncy
Nur Schreiben	waDtTNcCy
Vollzugriff	rwaDdxtTnNcCoy
Vollzugriff ohne ACL ändern	rwaDdxtTnNcoy

Standard-ACLs

Standardmäßig werden keine Berechtigungen vererbt. Jede neue Datei / Unterordner wird standardmäßig mit den Standard-ACLs initialisiert, die wie folgt lauten:

ACL Default

```
A::OWNER@:rwaDxtTnNcCoy
A::GROUP@:rxtncy
A::EVERYONE@:rxtncy
```

Dateien / Ordner mit einzelnen Nutzern freigeben

ACLs können sehr gut dazu verwendet werden, um bestimmte Dateien oder Ordnern mit bestimmten Nutzern / Nutzergruppen freizugeben. Eine vollständige ACL für einen Ordner mit zusätzlichen Berechtigungen für einen weiteren Nutzer und Vererbung für zukünftige Unterordner / Dateien könnte beispielsweise so aussehen:

ACL Nutzerfreigabe

```
A:fd:OWNER@:rwaDdxtTnNcCoy
A:fd:GROUP@:rxtncy
A:fd:EVERYONE@:tcy
A:fd:EigenerNutzername:rwaDxtncy
A:fd:NeuerNutzername:rwaDxtncy
```

Bestehende Regeln anpassen!

Beim Hinzufügen von Regeln mit Vererbung (`fd`) wie in diesem Beispiel erforderlich, ist es wichtig, dass auch die bestehenden Regeln um die Vererbungs-Flags `fd` erweitert werden. Andernfalls werden nur die Berechtigungen für die hinzugefügten Nutzer vererbt, der Eigentümer der Dateien hat anschließend keinen Zugriff mehr.

Außerdem muss neben der Regel für den neuen Benutzer ebenfalls eine Regel für den eigenen Benutzer hinzugefügt werden. Normalerweise ist der eigene Benutzer über `OWNER@` abgedeckt, wenn aber andere Nutzer in dem jetzt freigegebenen Verzeichnis Dateien anlegen, sind diese der Eigentümer (`OWNER@`) der neuen Dateien, und für den eigenen Benutzer existiert dann keine Regel mehr.

Siehe auch

Siehe auch: `man nfs4_acl`