Wie vergibt man Berechtigungen im Dateisystem?

Active Directory Gruppen

Funktion und Namensschema von AD-Gruppen im Kundenbereich der HHCL
Dieser Abschnitt beschreibt die Verwendung von AD-Gruppen in der Hamburg-Cloud-Umgebung. Aufgrund der Anforderungen, die in dieser hochstandardisierten Umgebung bestehen, gelten die hier dargestellten Regeln zur Verwendung, Verschachtelung und Namensgebung ausnahmslos in allen ab Veröffentlichung dieses Dokuments neu zu erstellenden Kundenumgebungen. Soweit möglich, werden vorhandene Umgebungen an dieses Schema angepasst.

Verwendung von AD-Gruppen

Im Kundenbereich der Hamburg-Cloud werden ALLE Berechtigungen, Beschränkungen, Ressourcenzuweisungen usw. über AD-Gruppen geregelt, soweit ein Active Directory verfügbar ist. Dies ist zum Beispiel nicht der Fall in DMZ-Bereichen. Hier müssen zwangsläufig lokale
Servergruppen verwendet werden. Eine Verschachtelung von Gruppen ist hier nicht erforderlich. Die Namensgebung sollte den hier aufgestellten Regeln weitgehend entsprechen.
In keinem Fall werden irgendwelche Zuordnungen direkt an User-Accounts gebunden.

Verfahren beim Zuordnen

Generell arbeiten wir nach dem von Microsoft eingeführten AGLP (Account-Global-Local-Permission)-Prinzip. Das heißt, dass User IMMER in globale Domänengruppen aufgenommen werden. Diese globalen Domänengruppen werden IMMER zu Mitgliedern lokaler Domänengruppen. Das Zuordnen von Ressourcen wird IMMER über die lokalen Domänengruppen geregelt.
Es gilt, dass es IMMER nur eine Verschachtelungsebene gibt. Daraus folgt, dass jede Zuordnung über zwei AD-Gruppen stattfindet.

Generelles Namensschema für AD-Gruppen

Für alle anzulegenden Gruppen gilt das im Folgenden vorgestellte Namensschema:

Anhand des Namens wird die Funktion einer Gruppe eindeutig ersichtlich.
Gruppen werden, soweit möglich, in englischer Sprache erstellt.
Die Namen dieser Gruppen bestehen IMMER aus diesen Teilen:

Global Groups:

1. Kundenkürzel (3 Stellen)
2. Funktionskürzel (max. 3 Stellen)

3. Beschreibung

Domain Local Groups

1. „LD“ – Kennzeichnung für „Local Domain Groups“
2. Kundenkürzel (3 Stellen) ersetzt in diesen Beispielen die Zeichen <CSN>
3. Funktionskürzel (max. 3 Stellen)
4. Beschreibung

Diese Teile werden IMMER durch einen Bindestrich getrennt.

Mögliche Funktionen von Gruppen

Die Funktionen, die globale Gruppen haben können, sind vielfältig. Man sollte jedoch vor der Einführung einer neuen Funktion ernsthaft überlegen, ob diese Funktion nicht bereits unter einem anderen Namen existiert oder ob diese neue Funktion auf Ebene der globalen Gruppen überhaupt erforderlich ist. Die folgende Tabelle zeigt die bisher definierten Funktionen für globale Gruppen:

Funktion	Beschreibung	Beispiel
LOC	Kundenstandort (User arbeitet dort)	<CSN>-LOC-HH
ORG	-Management à Geschäftsleitung -Accounting à Buchhaltung -HumanRes à Personalabteilung -Staff à Allg. Mitarbeiter ...	<CSN>-ORG-Managem

Die folgende Tabelle zeigt bisher definierte Funktionen von Local Domain Groups (LD):

Funktion	Beschreibung	Beispiel
LNK	Zuweisen einer Verknüpfung	LD-<CSN>-Lnk-AcrobatRe
FSm	Bearbeiten Dateien und Ordner erstellen, löschen und bearbeiten	LD-<CSN>-FSm-Public$--File
FSr	Lesen Ordner und Dateiinhalte lesen	LD-<CSN>-FSr-Public$--File
FSf	Vollzugriff Kompletter Zugriff incl. der Möglichkeit Berechtigungen zu verändern.	LD-<CSN>-FSf-Public$--File

Ordner und Dateien anzeigen, jedoch keinen Zugriff auf den Inhalt einer Datei

Erläuterungen zu den Gruppenfunktionen

Es wird deutlich, dass mit den Global Groups in erster Linie das Unternehmen abgebildet werden soll.

Dies soll sowohl die Handhabung vereinfachen, als auch Fehler verhindern.

Es ist geplant, dass unsere Kunden und auch der Service Desk, Ressourcen über ein Webportal selbst zuweisen können. Dementsprechend ist davon auszugehen, dass die Personen, die hierfür verantwortlich sind, zwar weniger tief in der Technik stecken, dafür aber wissen, welcher Mitarbeiter in welcher Funktion im Unternehmen eingesetzt wird.

Alle Einstellungen (Ressourcen, Berechtigungen, Laufwerke etc.) sind an Local Domain Groups gebunden. Dementsprechend werden die Global Groups nun zu Mitgliedern der entsprechenden Local Domain Groups.

Empfehlungen für den Aufbau eines filebasierten Datenablagesystems

Es gibt sicher viele Ansätze einer strukturierten Datenablage. In diesem Kapitel soll unser favorisiertes System beschrieben werden. Dieses System hat folgende Vorteile:

- Einfache, wiederverwendbare Struktur
- An Unternehmensstrukturen anpassbar
- Flacher Aufbau
- Übersichtliche, sichere, Berechtigungsstruktur

Voraussetzung für eine sinnvolle Nutzung dieses Systems, ist der Einsatz von ABE (access based enumeration).

Der hier beschriebene Aufbau des Filesystems startet im Root eines Laufwerks oder eines DFS-Shares (sollten keine Gründe gegen die Nutzung von DFS sprechen, empfehlen wir grundsätzlich dessen Nutzung).

Die Berechtigung auf einzelne Ordner werden grundsätzlich über AD-Gruppen abgebildet. Einzelheiten hierzu bitte unter Mögliche Funktionen von Gruppen nachlesen.

[root]

Data

Profiles

Homes

Die Namen der Ordner sind selbsterklärend. An dieser Stelle soll nur auf den Folder „Data“ eingegangen werden.

Die Struktur unterhalb von Data bildet die Abteilungen eines Unternehmens ab. Dabei gibt es pro Abteilung mindestens zwei Ordner. Der erste Ordner bietet Ablagemöglichkeiten für alle Mitarbeiter der Abteilung. Der zweite Ordner ist der Abteilungsleitung vorbehalten.

Zusätzlich gibt es Ordner für übergreifenden Zugriff aller Mitarbeiter. Auch hier kann parallel ein

„Leitungsordner“ erstellt werden, wenn dies erforderlich ist. Hier ein Beispiel:

Accounting

AccountingHead

HumanRes

HumanResHead

Worker

WorkerHead

Management

ManagementHead

Public

PublicHead

Für jeden Ordner werden zwei Gruppen erstellt. Eine Gruppe berechtigt zum Lesen, die zweite Gruppe erhält Modify-Rechte.

Geht man davon aus, dass es innerhalb einer Abteilung keine „Geheimnisse“ gibt,

reicht diese Ordnerstruktur aus. Andernfalls können parallel weitere „Abteilungen“ erstellt werden. Wir gehen weiter davon aus, dass nun das Data-Share als Laufwerk (Beispiel F:\) erstellt wird, und dies jedem Mitarbeiter bereitgestellt wird.

Im einfachsten Fall sähe dies nun für einen Mitarbeiter der Abteilung Worker wie folgt aus:

F:\Worker

F:\Public

Der Leiter der Worker-Abteilung sieht dies:

F:\Worker

F:\WorkerHead

F:\Public

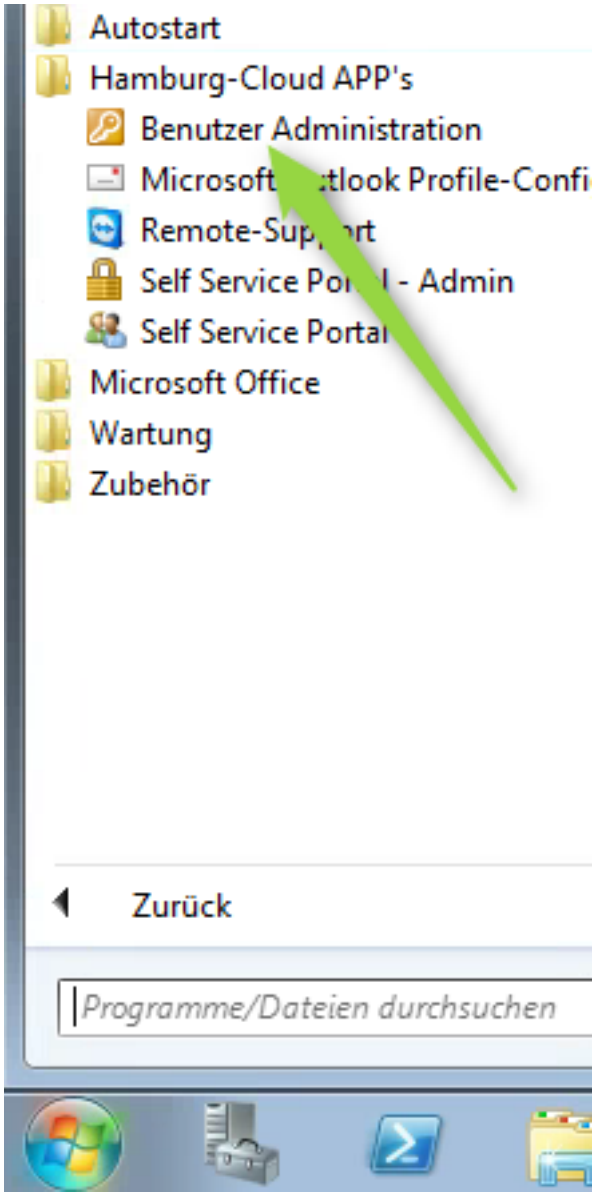
Auf diese Art und Weise kann jede beliebige Sichtbarkeit auf jeden Ordner dargestellt werden. Es werden keine zusätzlichen Laufwerksbuchstaben benötigt. Die Berechtigungszuweisung kann vom Kunden selbst durchgeführt werden. Änderungen innerhalb der Belegschaft oder auch in der Struktur des Unternehmens sind einfach abbildbar.

Beim Aufbau der Berechtigungsstruktur ist ebenfalls Kapitel Active Directory Gruppen heranzuziehen.

Gruppen-Verwaltung

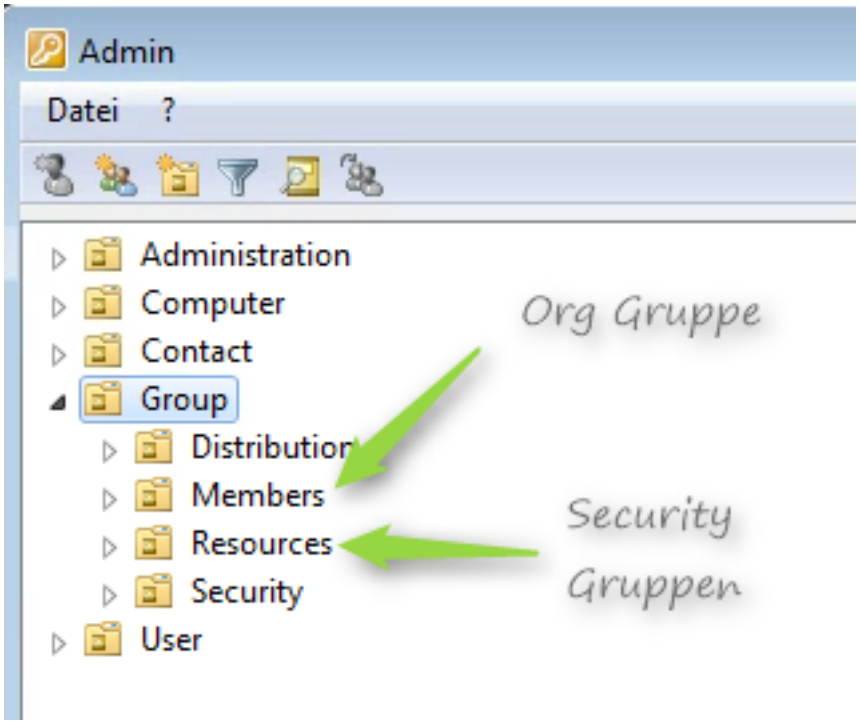
Um die benötigten Gruppen im System anlegen zu können, muss der Verwaltungsbenutzer Mitglied der Gruppe LR-<CSN>-ADM-Group und LR-<CSN>-ADM-Admin-Shares sein.

Diese Gruppenmitgliedschaften sorgen dafür, dass im Startmenü das entsprechende Symbol erscheint, Sie Berechtigungen besitzen um NTFS-Berechtigungen zu setzen und Sie Zugriff auf die Verwaltung von Gruppen haben.



Organisationseinheiten (OU’s)

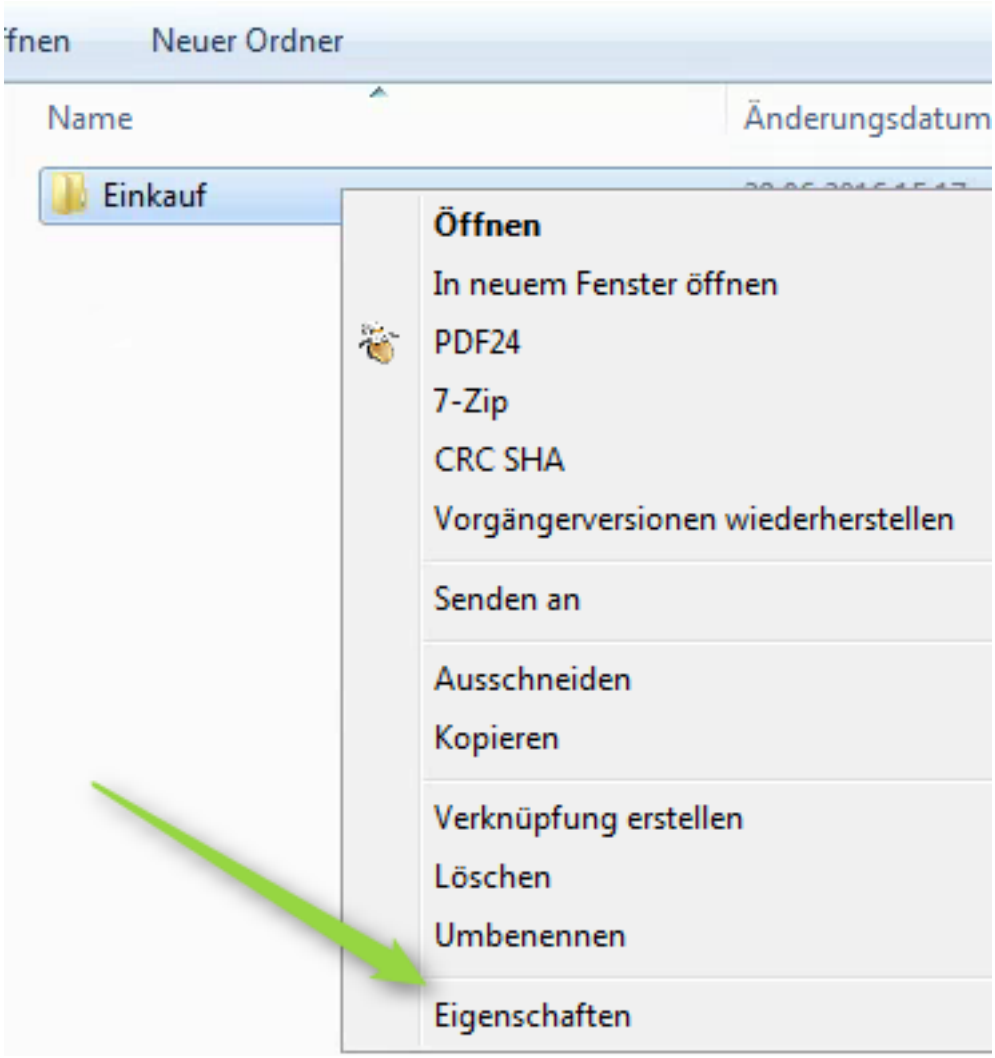
Die OU Struktur jedes Kunden, sieht wie folgt aus:



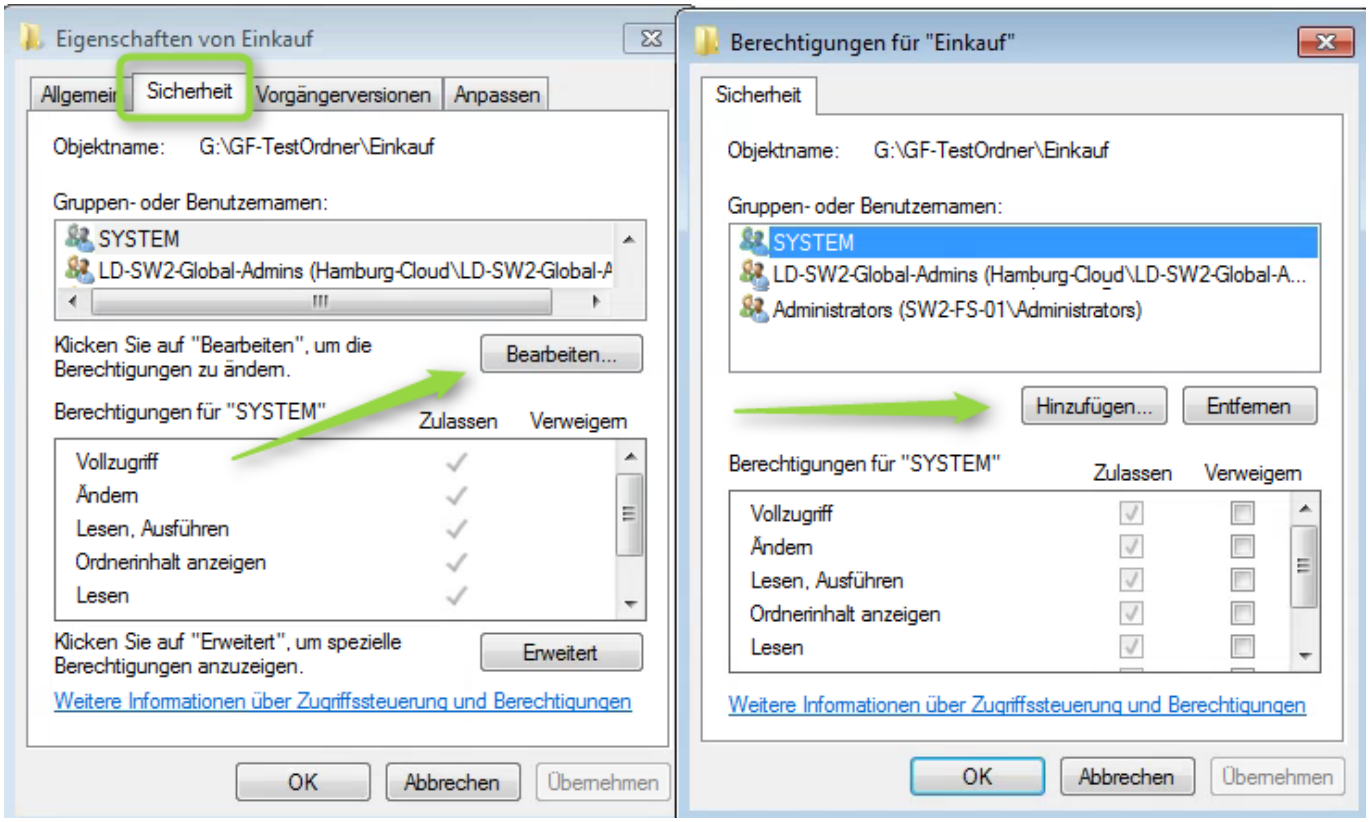
Innerhalb der OU Members werden die sogenannten ORG-Gruppen und innerhalb der OU Resources die Security-Gruppen angelegt. Wie das Namenskonzept für die entsprechenden Gruppen aussieht, lesen Sie bitte weiter oben in diesem Artikel nach.

NTFS-Berechtigungen

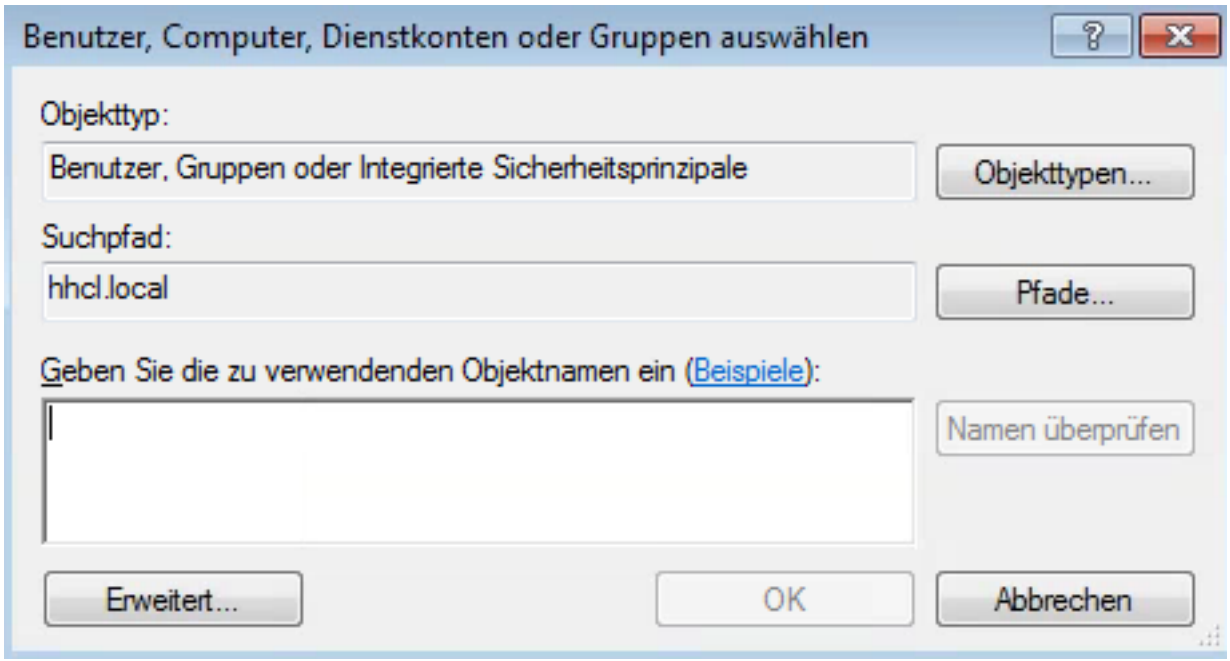
Wenn ihr Benutzer Mitglied der Gruppe LR-<CSN>-ADM-Admin-Shares ist, dann haben Sie die Möglichkeit die Berechtigungen auf NTFS-Ebene über eine Citrix XenApp-Sitzung selbst durchzuführen. Sie öffnen also den Explorer innerhalb des Smart Workplaces und navigieren zu dem Ordner, den Sie berechtigen wollen, aktivieren auf diesem Ordner das Kontextmenü und wählen Eigenschaften aus.



Anschließend wählen Sie die Registerkarte Sicherheit aus und klicken auf Hinzufügen.



Über das Suchfenster, suchen Sie nach der gewünschten LOKALEN Gruppe LD-<CSN>-FS und wählen diese Gruppen aus.



Berechtigungen

LD-<CSN>-FSl Gruppen werden mit dem Recht Ordnerinhalt anzeigen, die Gruppe LD-<CSN>-FSm mit dem Recht Ändern und die Gruppe LD-<CSN>-FSr mit dem Recht Lesen berechtigt.

Die Gruppen mit der Bezeichnung LD-<CSN>-FSf sollten nur in absoluten Notfällen

genutzt werden, erhalten dann das Recht Vollzugriff.

Zu beachten sind bei Berechtigungen immer, dass innerhalb des kompletten Verzeichnisbaumes mindestens das Recht Ordnerinhalt anzeigen existieren muss, damit ein Benutzer in die Unterordner navigieren kann.

Eindeutige ID: #1102