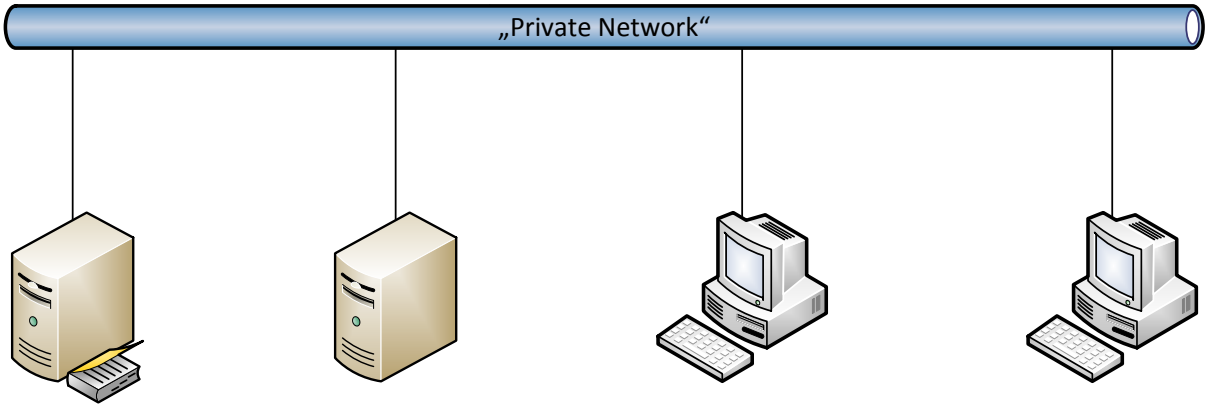
Inhalt

Szenario Beschreibung



LON-DC1.adatum.com	LON-SVR1.adatum.com	LON-CL1.adatum.com	LON-CL2.adatum.com
NIC1: 172.16.0.10/16	NIC1: 172.16.0.21/16	NIC1: 172.16.0.50/16	NIC1: 172.16.0.51/16
DC,GC,DNS,DHCP,CA,IIS	DHCP,IIS,FS,ISCSi	{Manager-PC}	{Standard-PC}

- Lon-CL1 ist als Computerkonto Mitglied in der AD-Gruppe WKS-Manager, Lon-CL2 gehört nicht zu dieser Gruppe
- Benutzerkonten
  - Aidan ist Manager
  - Allie gehört zur Abteilung Research
- Freigaben auf Server Lon-SVR1:
  - Docs: enthält teilweise vertrauliche Dokumente
  - Research: enthält Dokumente für die Abteilung Research

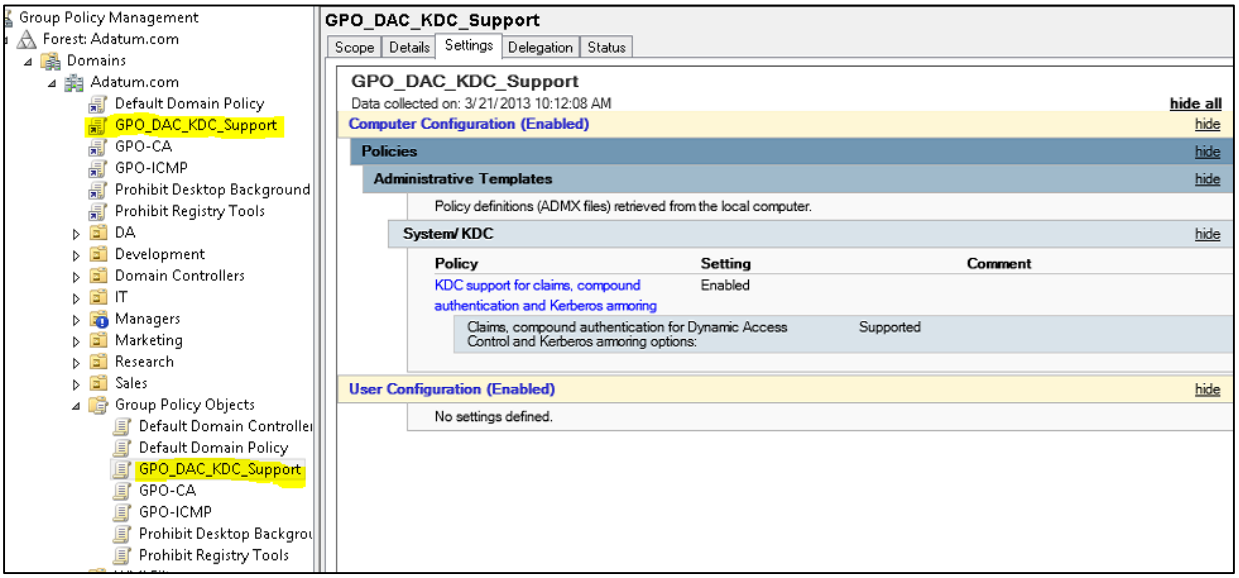
Aufgabenstellung

- Die Freigabe \\lon-svr1\research soll nur für Benutzer mit dem AD-Attribut Department=Research zur Verfügung stehen.
- Die Dokumente unter \\lon-svr1\docs, welche das Wort „secret“ enthalten, sollen nur für Benutzer verfügbar sein, die der Abteilung „Managers“ angehören, wenn diese auf Computern angemeldet sind, die der Sicherheitsgruppe „WKS-Managers“ angehören.
- Es soll eine benutzerdefinierte Meldung anstelle „Zugriff verweigert“ angezeigt werden.

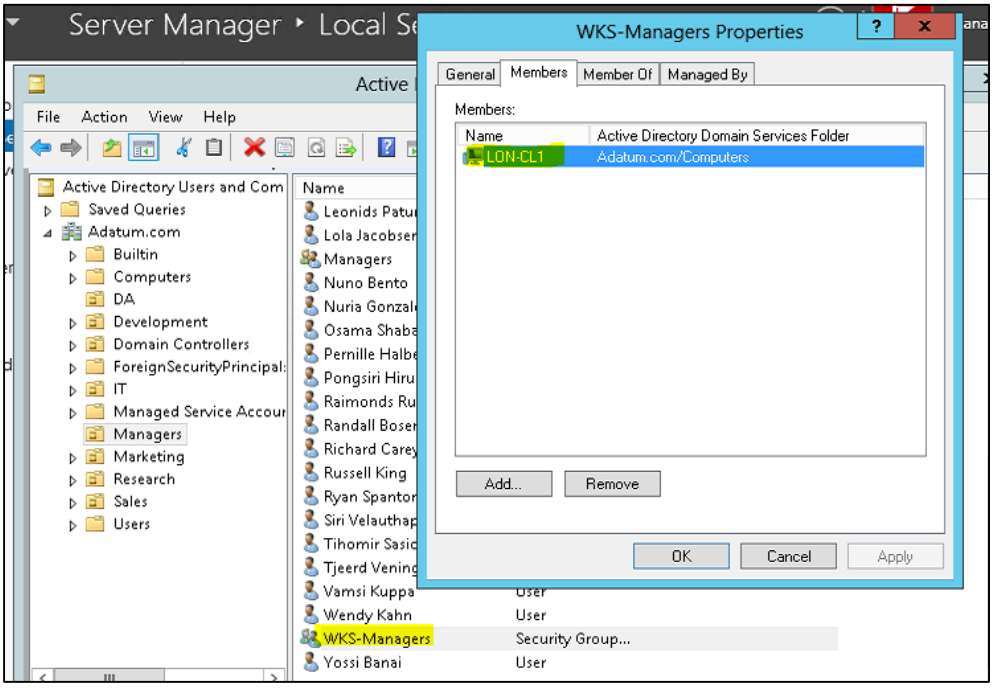
Konfiguration

Vorbereitung im Active Directory

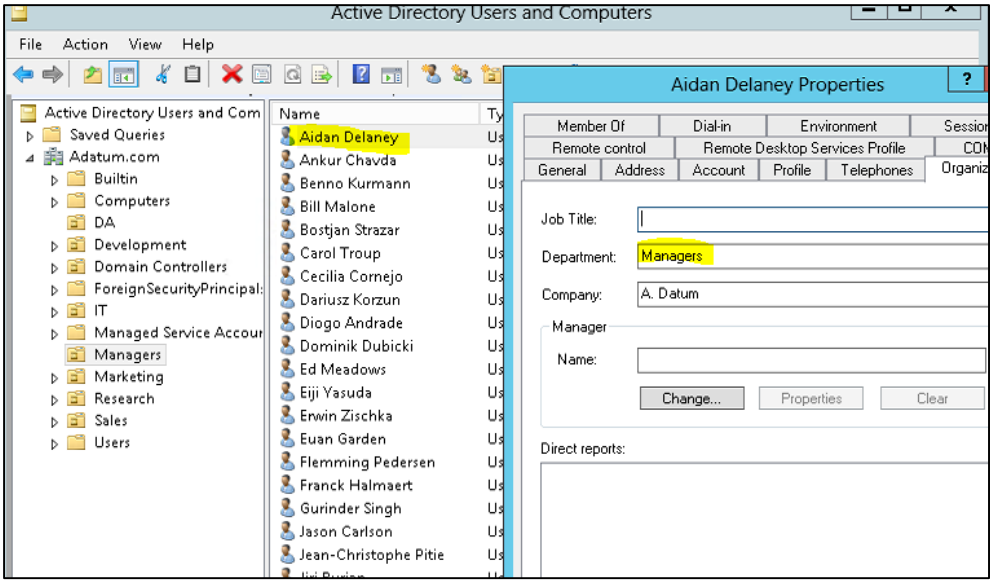
- Neue GPO für die Aktivierung des KDC-Claim-Supportes erstellen und auf LON-SVR1 anwenden:

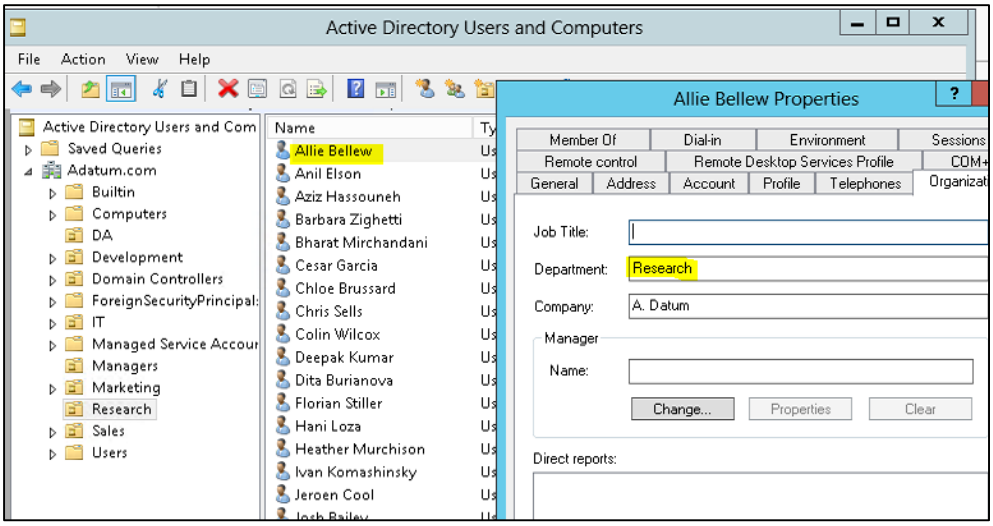


- Eine Gruppe für die Manager-PCs erstellen:

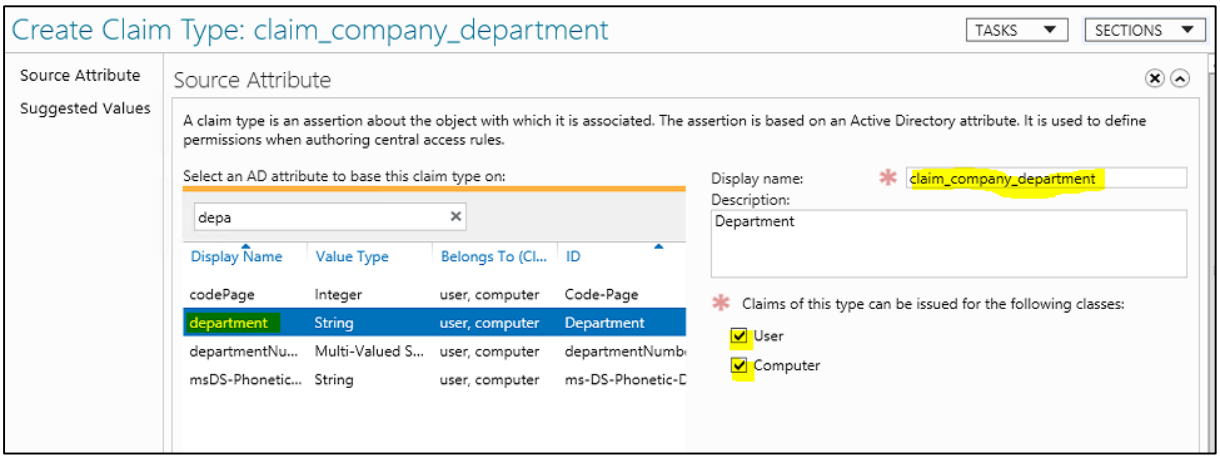


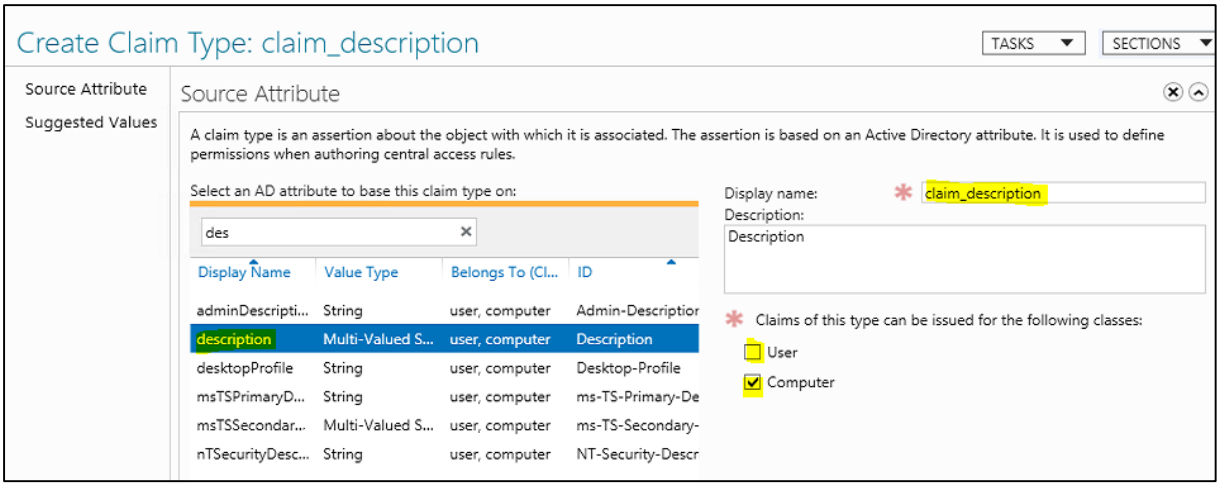
- Kontrolle der Benutzer Aidan und Allie:



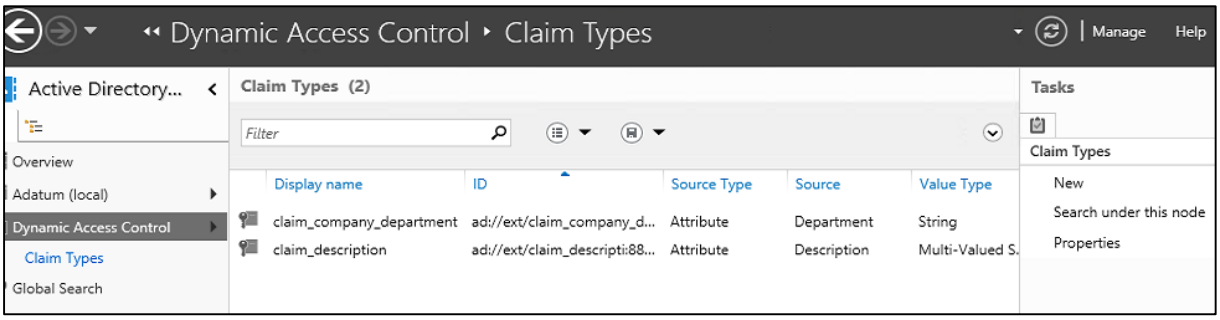


- Erstelle Claims im Active Directory Administrative Center:

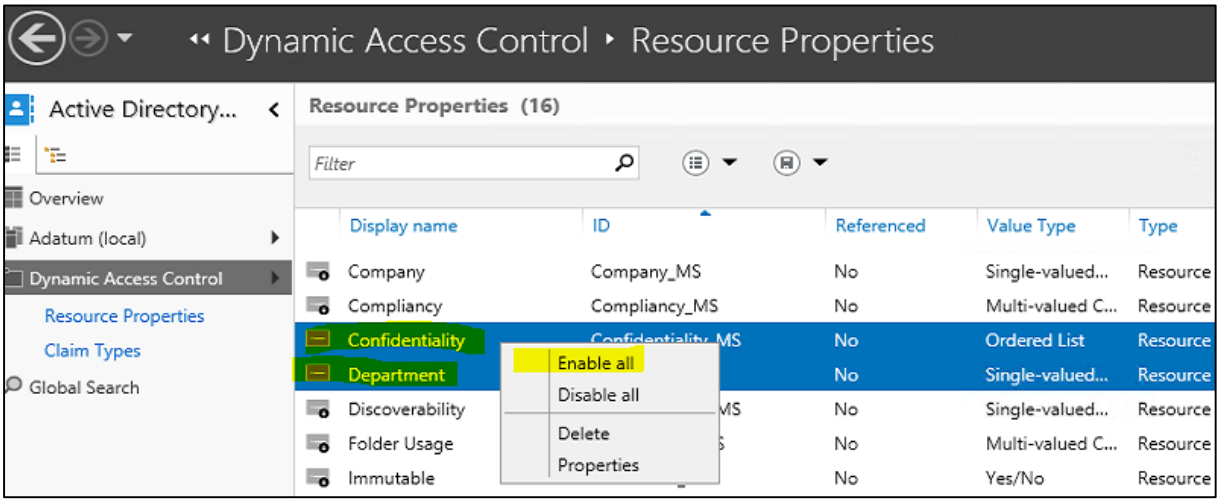




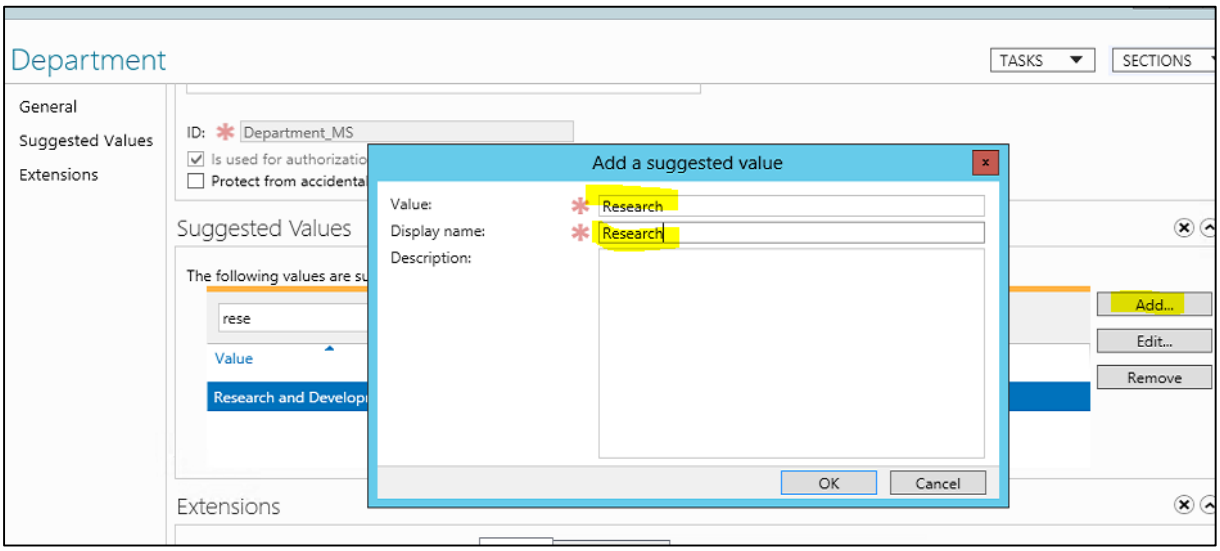
Ergebnis:



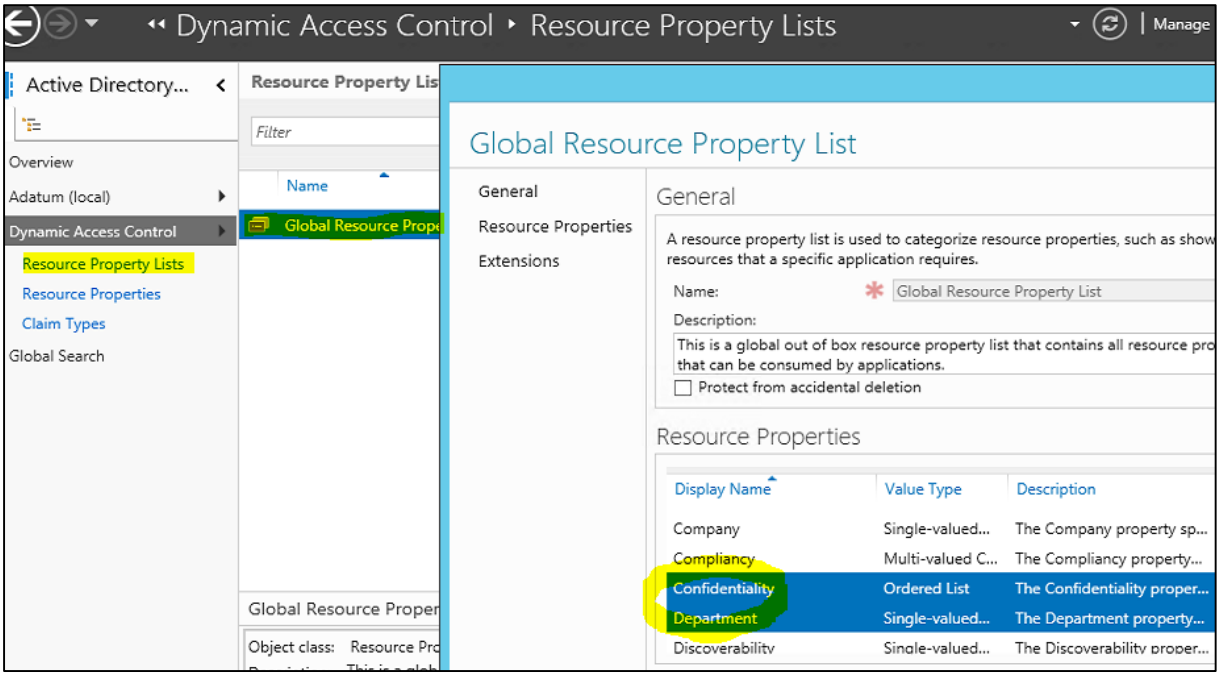
- Aktiviere Ressource-Properties für die Fileserver:



- Füge bei der Ressource-Property “Department” einen Auswahlwert an:

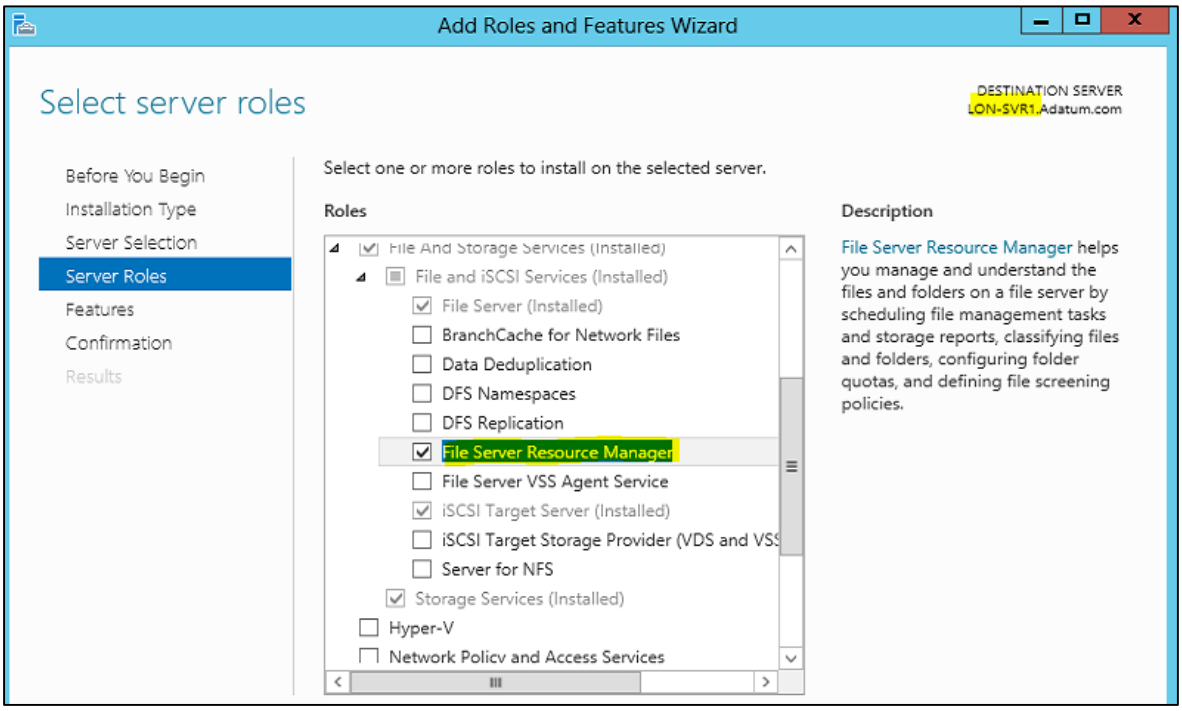


- Kontrolliere, ob die beiden Ressource Properties in der Global Ressource Property List veröffentlicht werden:

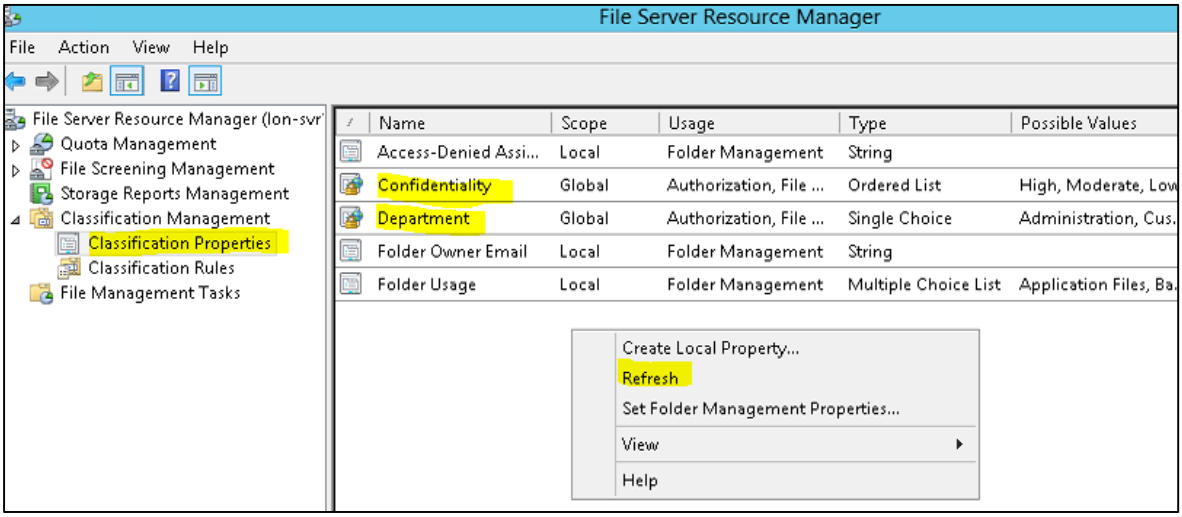


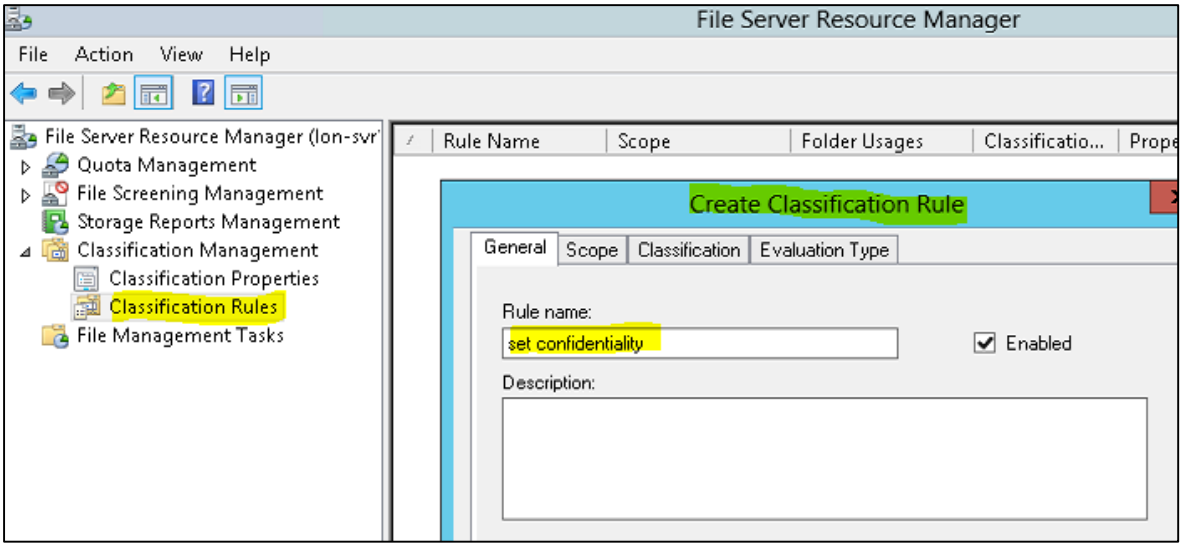
Vorbereitung auf dem Fileserver

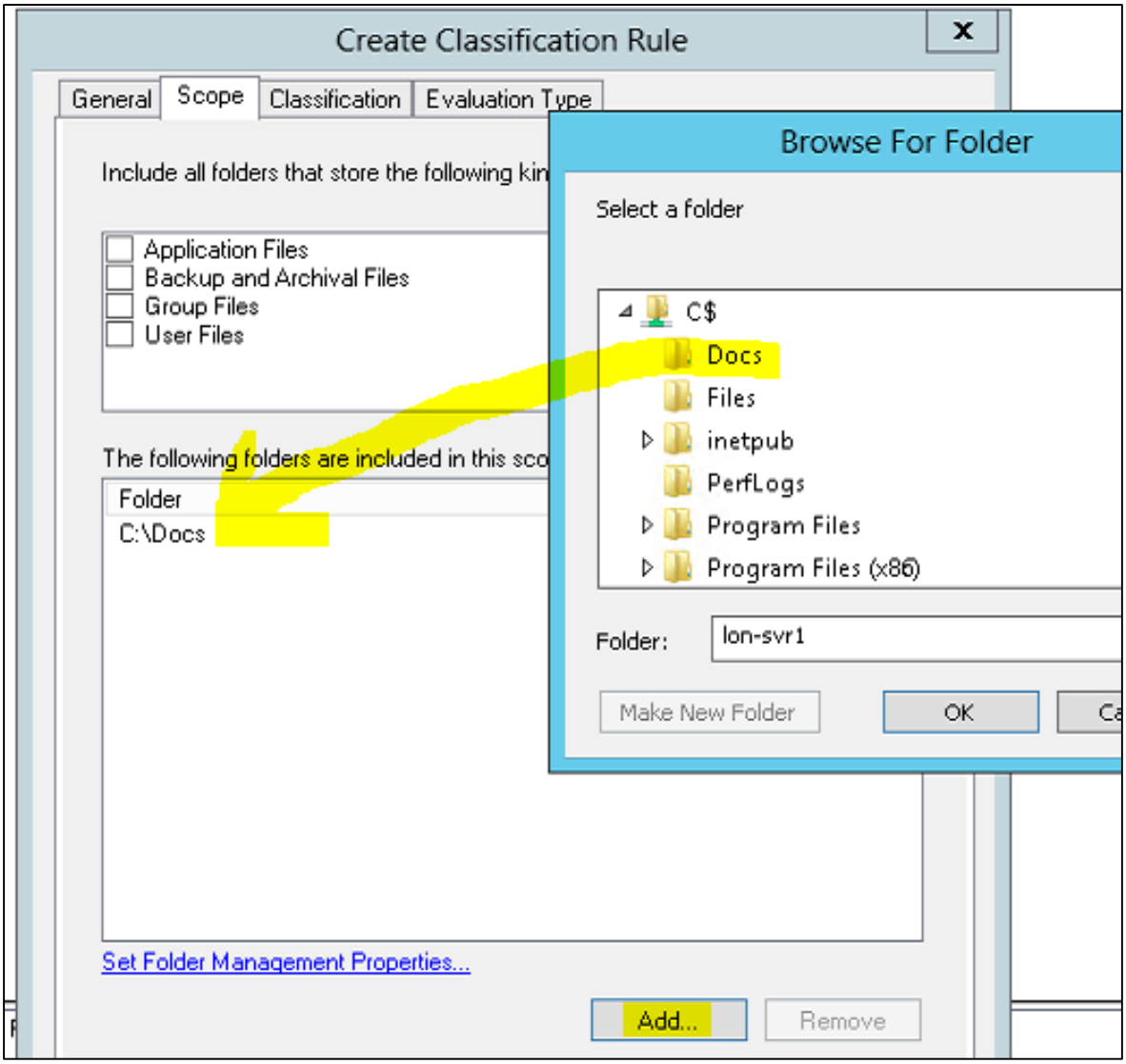
- Installiere auf LON-SVR1 den FSRM:

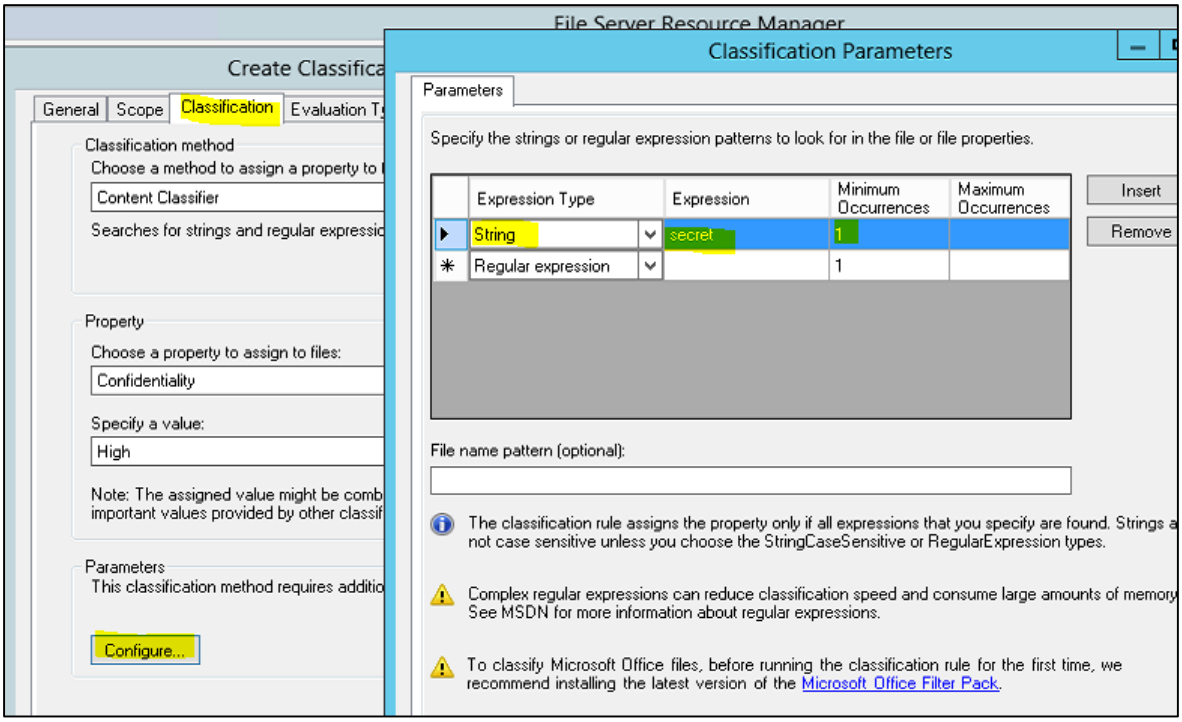


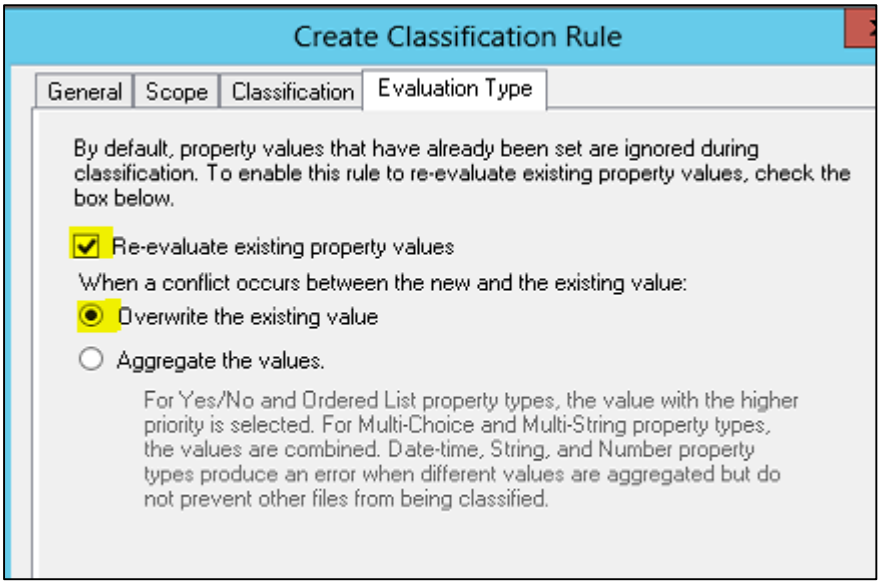
- Konfiguriere File-Klassifizierung auf dem Fileserver mit FSRM (ggf. gpupdate /force):



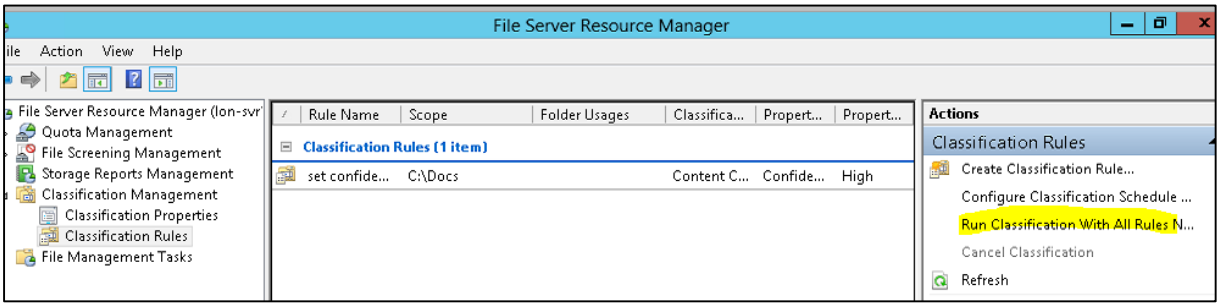

File Server Resource Manager
File Action View Help
File Server Resource Manager (lon-svr
Quota Management
File Screening Management
Storage Reports Management
Classification Management
Classification Properties
Classification Rules
File Management Tasks
Rule Name
Scope
Folder Usages
Classificatio...
Create Classification Rule
General
Scope
Classification
Evaluation Type
Rule name:
set confidentiality
Enabled
Description:


Create Classification Rule
General
Scope
Classification
Evaluation Type
Include all folders that store the following kin
Application Files
Backup and Archival Files
Group Files
User Files
The following folders are included in this sco
Folder
C:\Docs
Set Folder Management Properties...
Add...
Remove
Browse For Folder
Select a folder
C$
Docs
Files
inetpub
PerfLogs
Program Files
Program Files (x86)
Folder:
lon-svr1
Make New Folder
OK

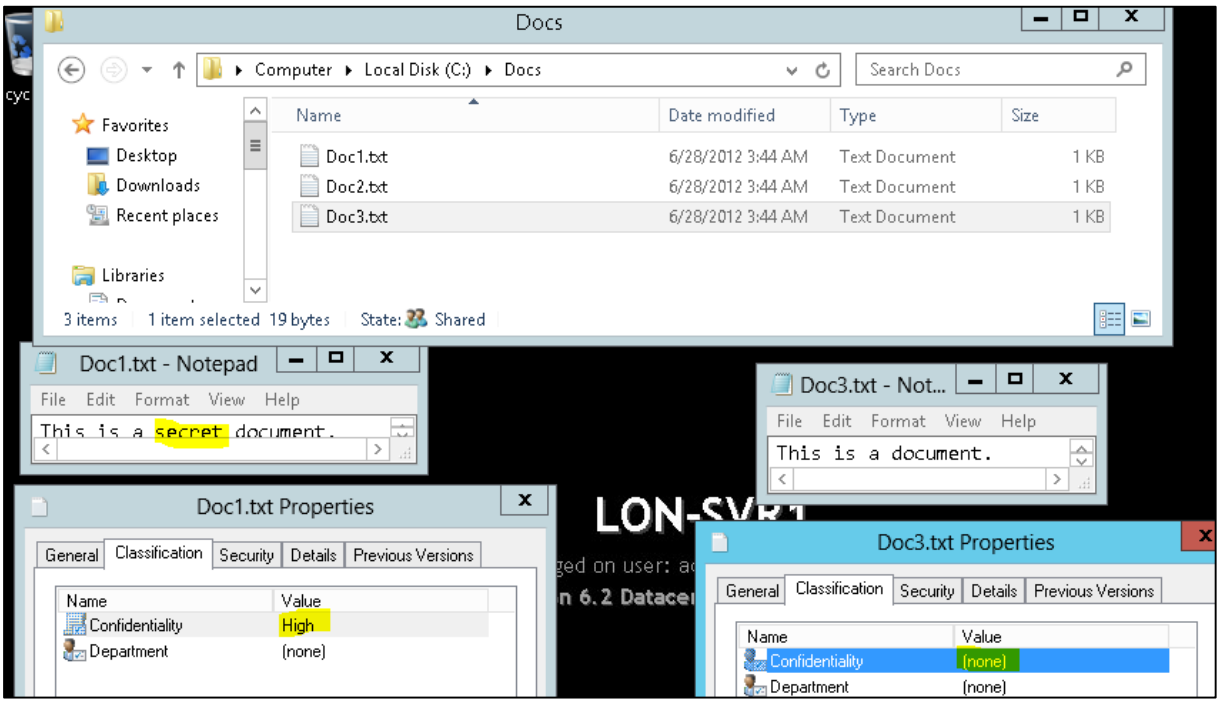




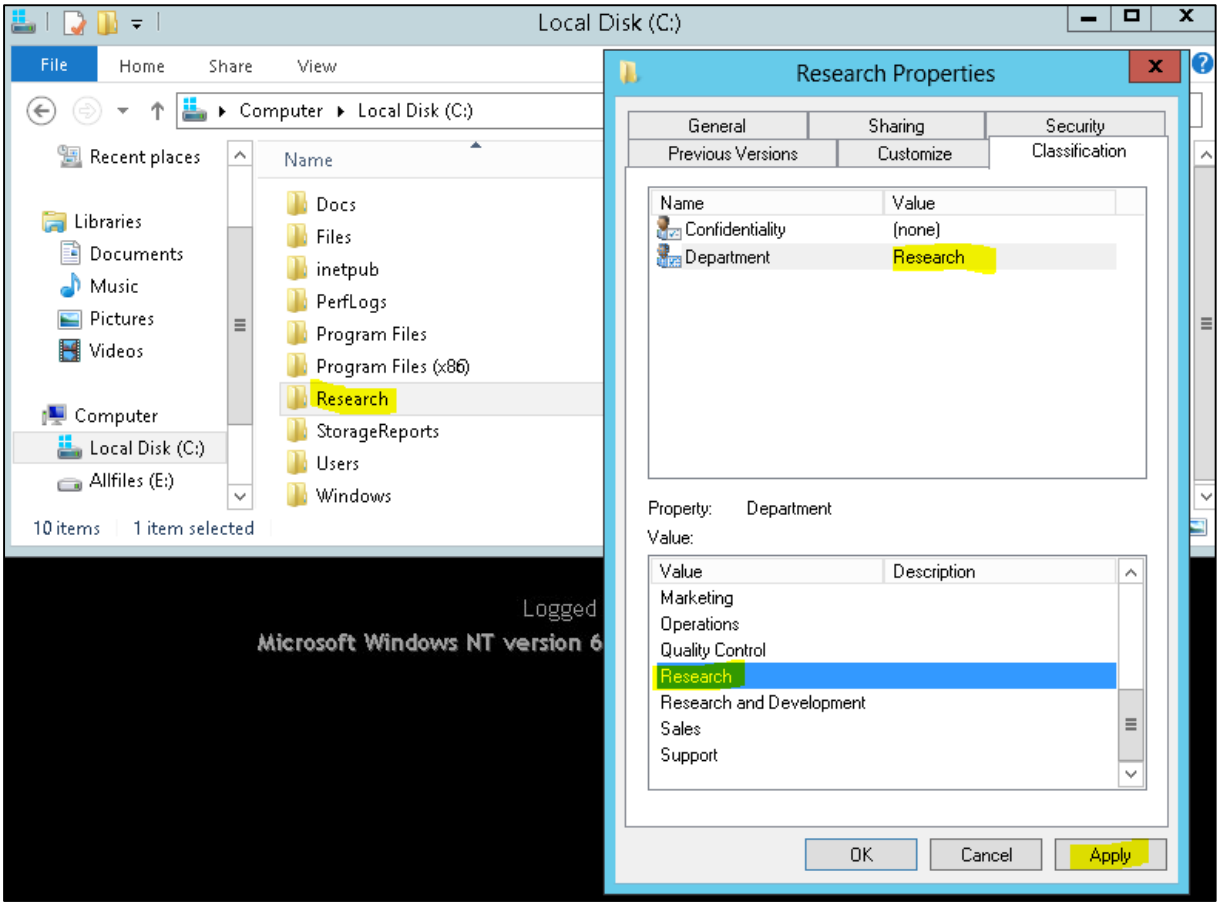
- Starte manuelle Klassifizierung:



- Kontrolliere Klassifizierungsergebnis:

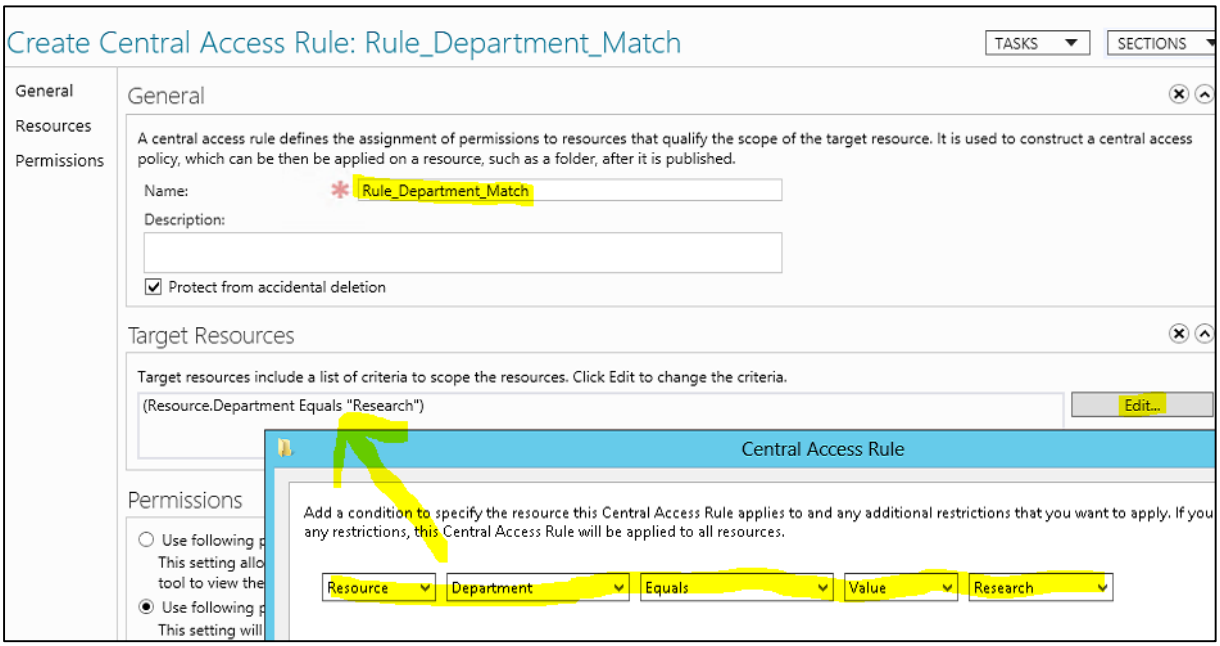


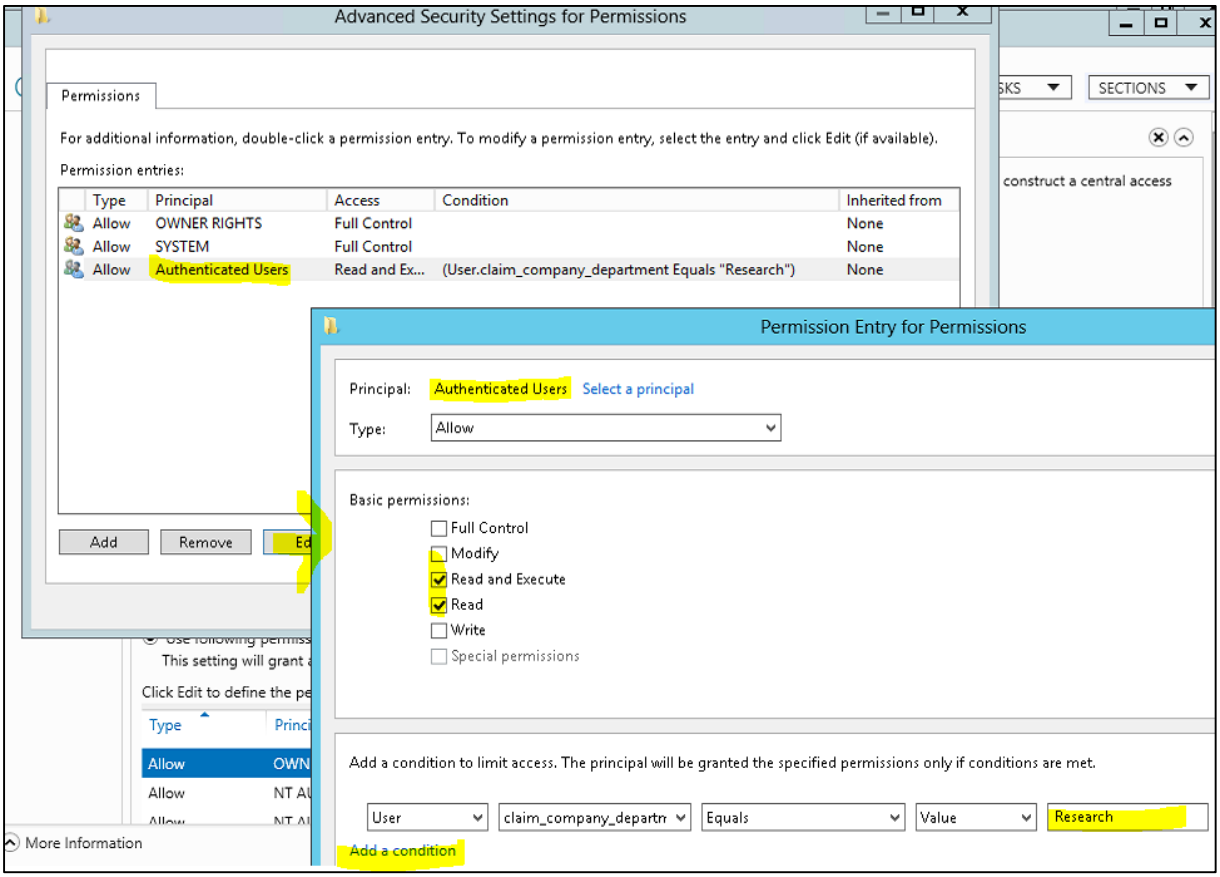
- Konfiguriere das Department-Flag für den Ordner Research auf Lon-SVR1:



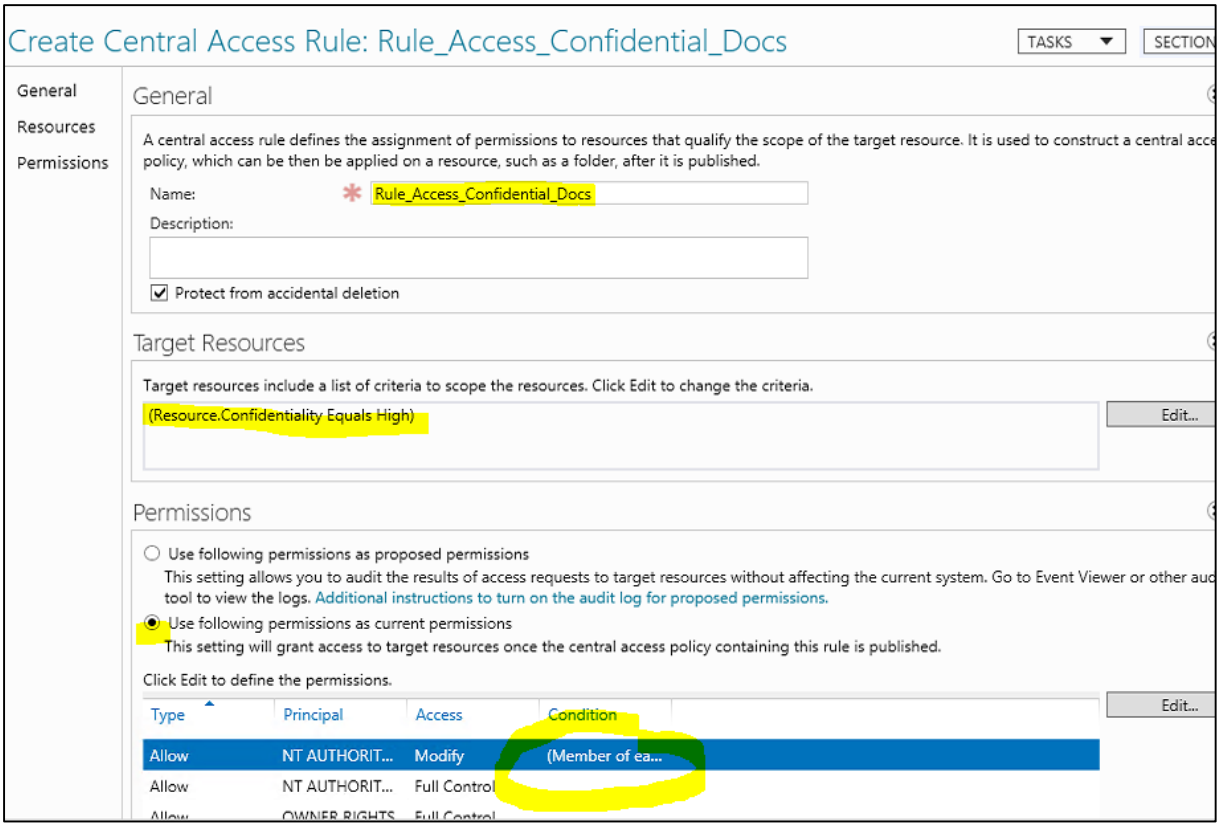
Erstelle zentrale Zugriffsregeln im Active Directory

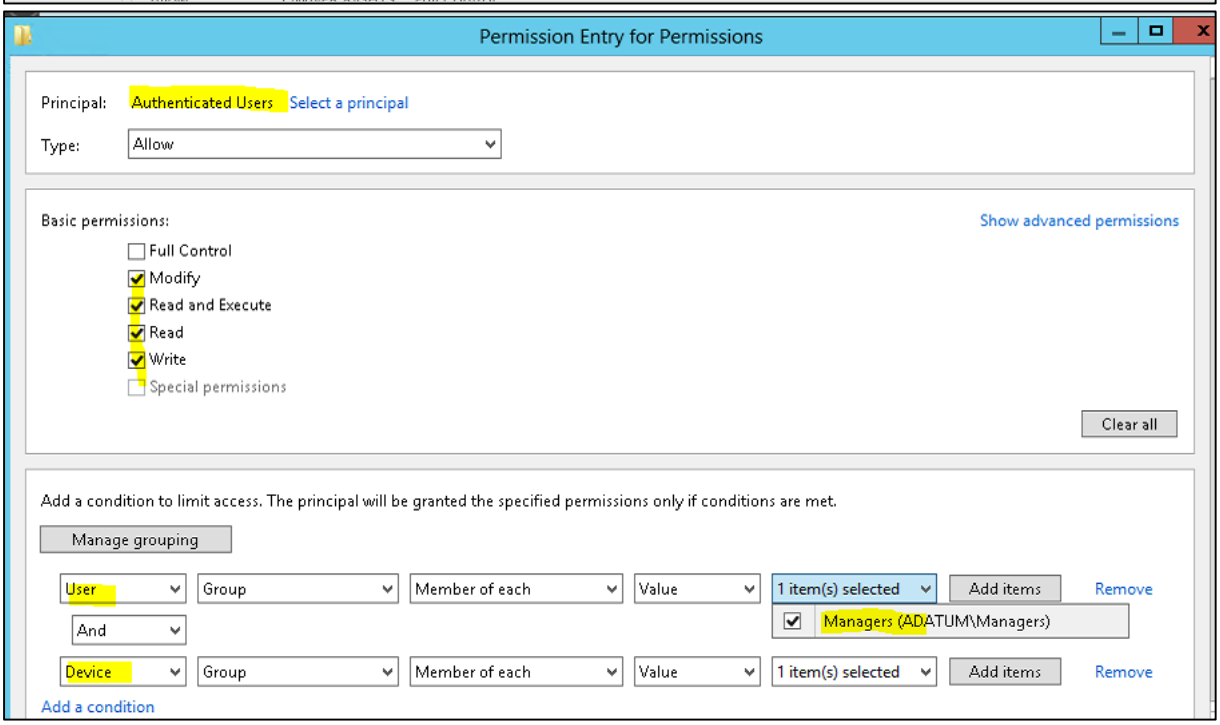
- Erstelle zentrale Zugriffsregel für die Department-Anforderung:





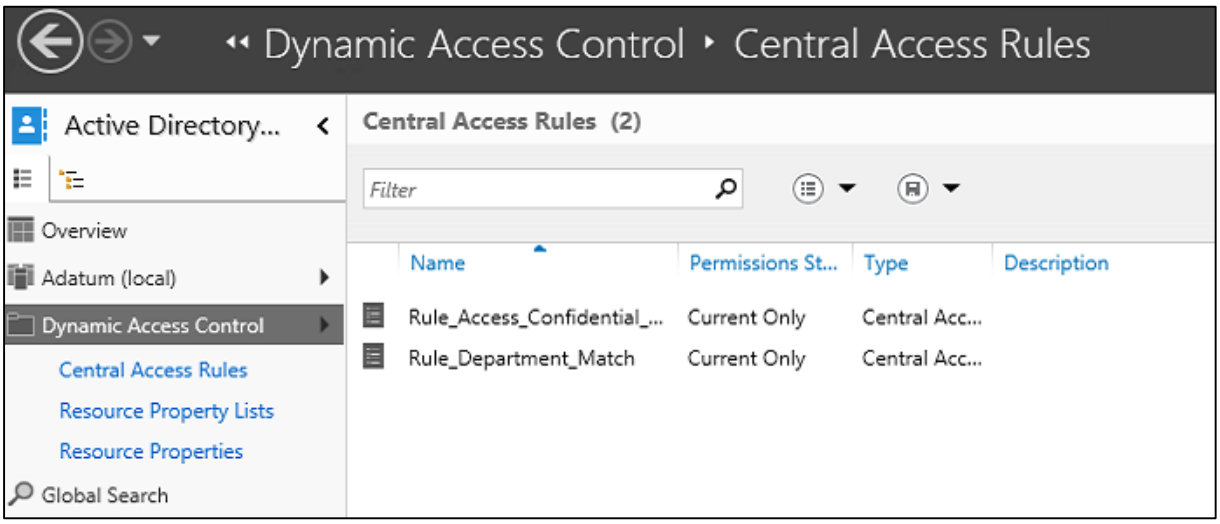
- Erstelle Regel für vertrauliche Dokumente:


Create Central Access Rule: Rule_Access_Confidential_Docs
TASKS
SECTION
General
Resources
Permissions
General
A central access rule defines the assignment of permissions to resources that qualify the scope of the target resource. It is used to construct a central acce
policy, which can be then be applied on a resource, such as a folder, after it is published.
Name:
Rule_Access_Confidential_Docs
Description:
Protect from accidental deletion
Target Resources
Target resources include a list of criteria to scope the resources. Click Edit to change the criteria.
(Resource.Confidentiality Equals High)
Edit...
Permissions
Use following permissions as proposed permissions
This setting allows you to audit the results of access requests to target resources without affecting the current system. Go to Event Viewer or other auc
tool to view the logs. Additional instructions to turn on the audit log for proposed permissions.
Use following permissions as current permissions
This setting will grant access to target resources once the central access policy containing this rule is published.
Click Edit to define the permissions.
Edit...
Type
Principal
Access
Condition
Allow
NT AUTHORIT...
Modify
(Member of ea...
Allow
NT AUTHORIT...
Full Control


Permission Entry for Permissions
Principal:
Authenticated Users
Select a principal
Type:
Allow
Basic permissions:
Show advanced permissions
Full Control
Modify
Read and Execute
Read
Write
Special permissions
Clear all
Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.
Manage grouping
User
Group
Member of each
Value
1 item(s) selected
Add items
Remove
Managers (ADATUM\Managers)
And
Device
Group
Member of each
Value
1 item(s) selected
Add items
Remove
Add a condition

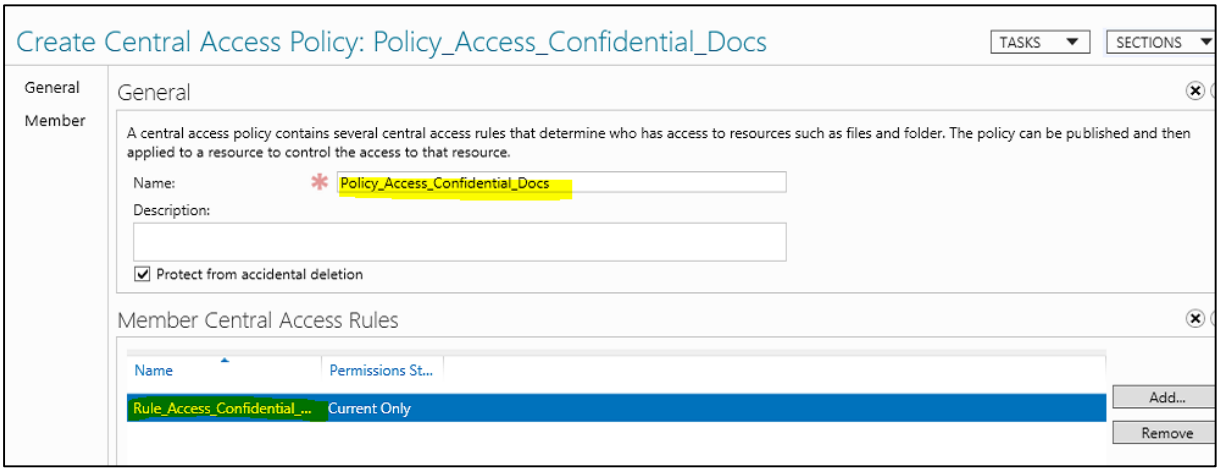

Device
Group
Member of each
Value
1 item(s) selected
Add items
Remove
Add a condition
WKS-Managers (ADATUM\WKS-Man...

- Ergebnis:

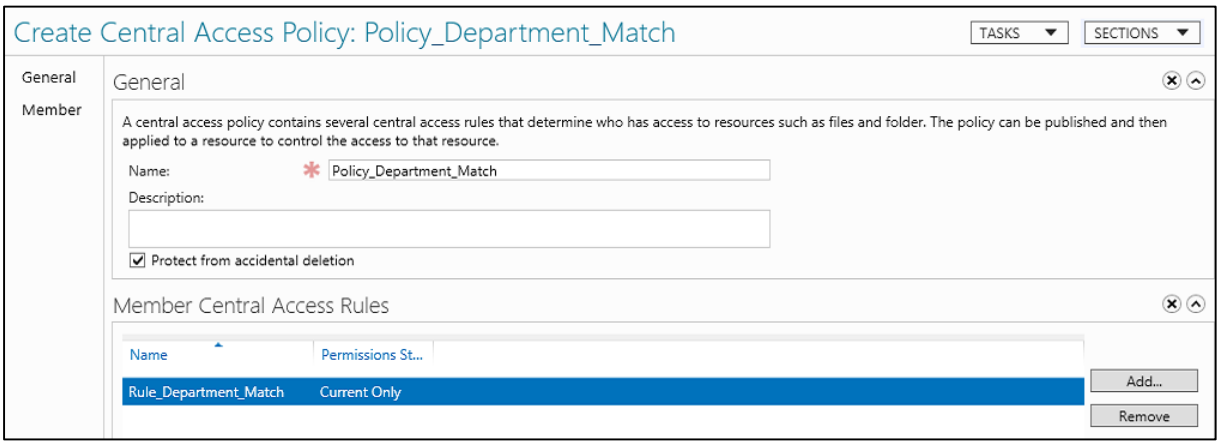


Erstelle zentrale Zugriffsrichtlinien im Active Directory

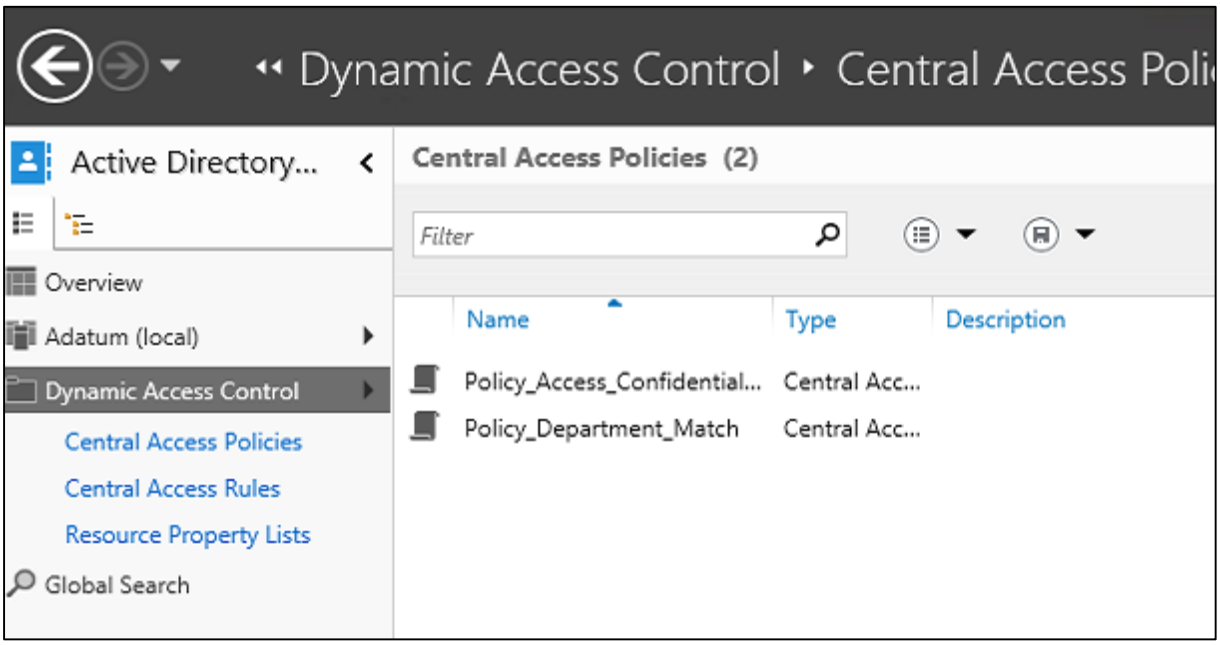
- Erstelle Richtlinie für die vertraulichen Dokumente:



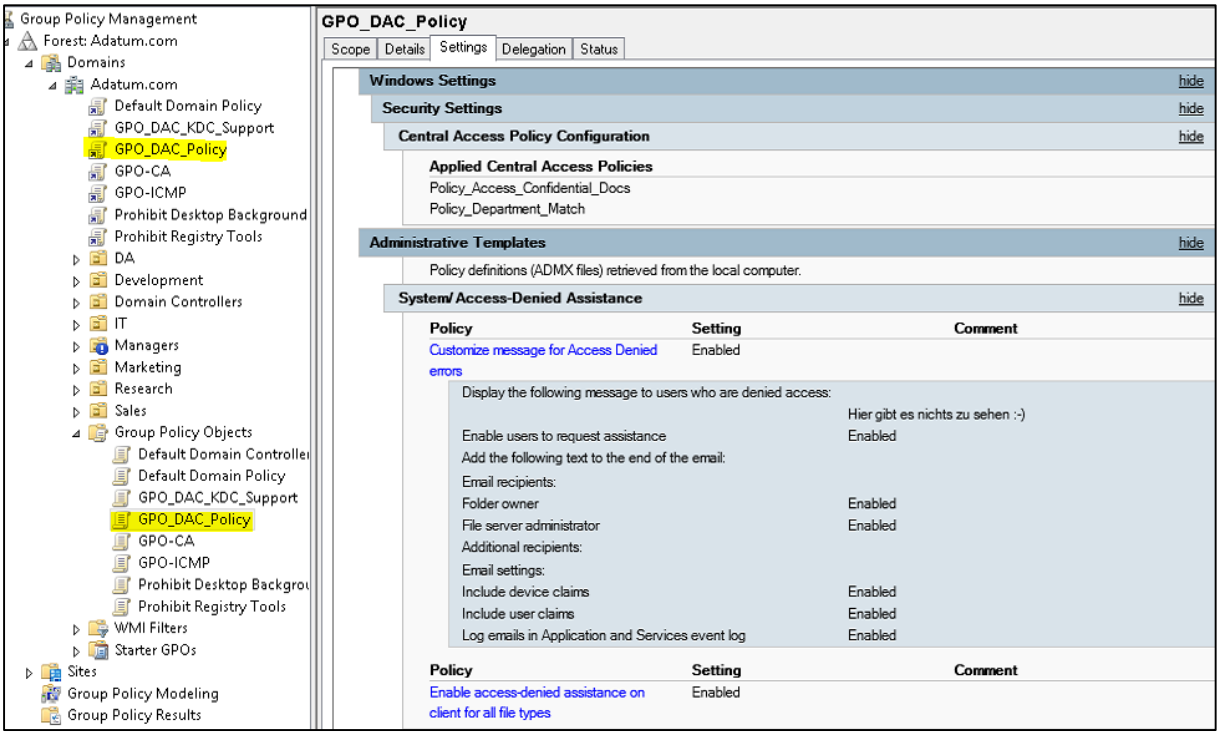
- Erstelle Richtlinie für die Department-Anforderung



Ergebnis:

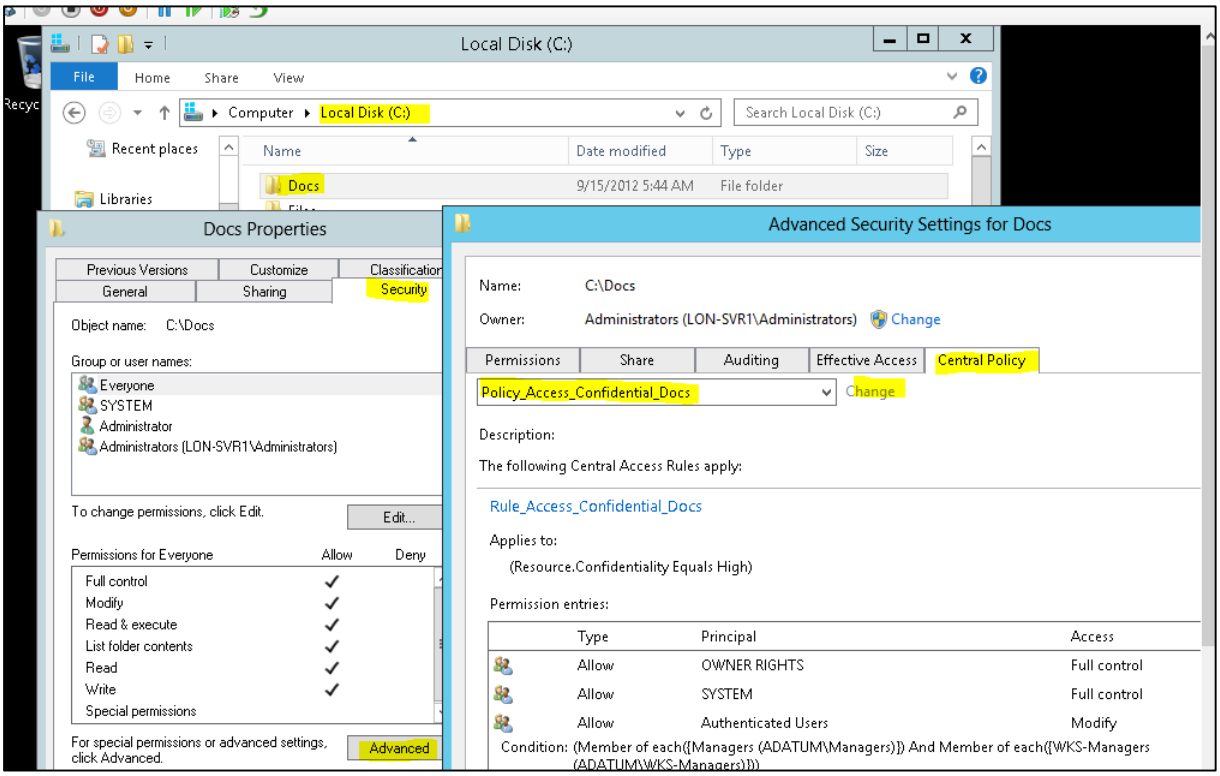


- Veröffentliche die neuen Richtlinien mit einer GPO auf dem Fileserver:

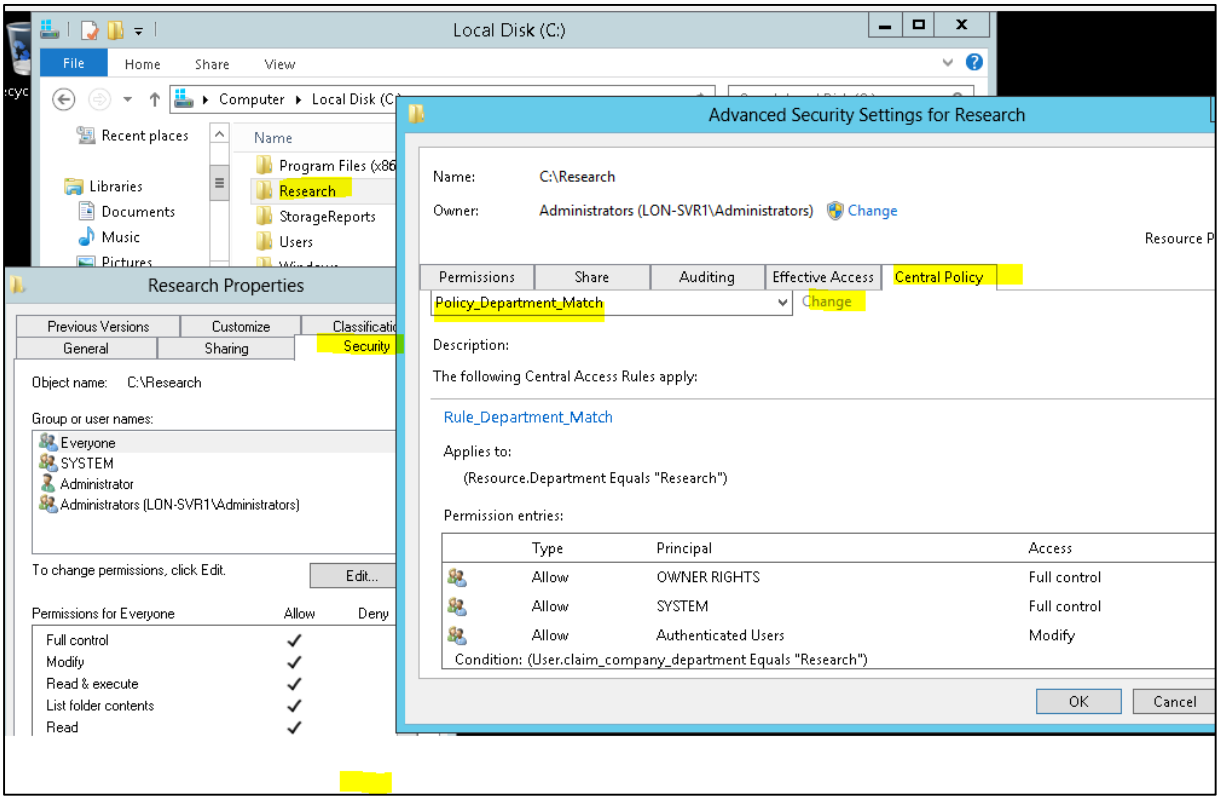


Konfiguriere Zugriffsrichtlinien auf den Freigabeordnern:

- Konfiguriere Zugriff für vertrauliche Dokumente:



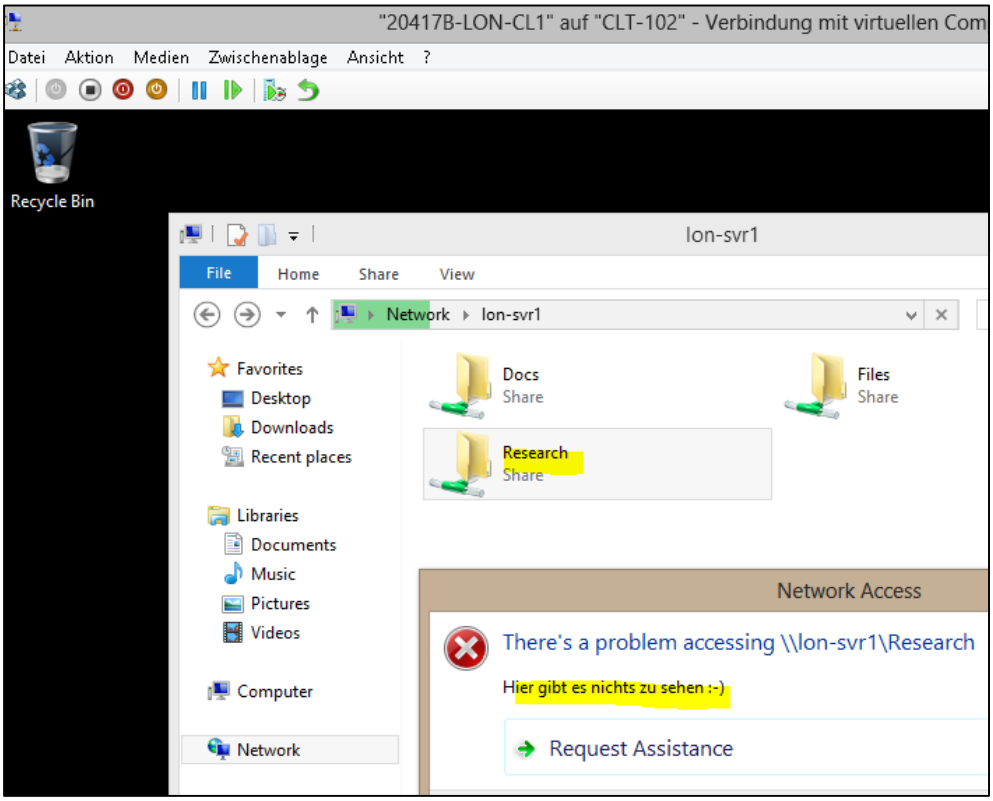
- Konfiguriere Zugriff für das Department Research:



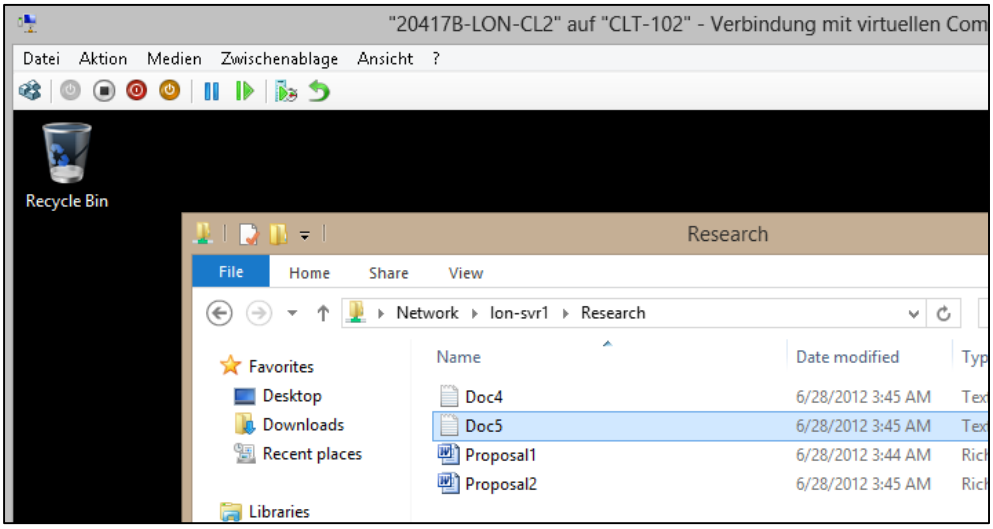
Testphase

Test für die Department-Anforderung

- Zugriff von Aiden (Department = Managers) auf \\lon-svr1\research (Client ist dabei egal):

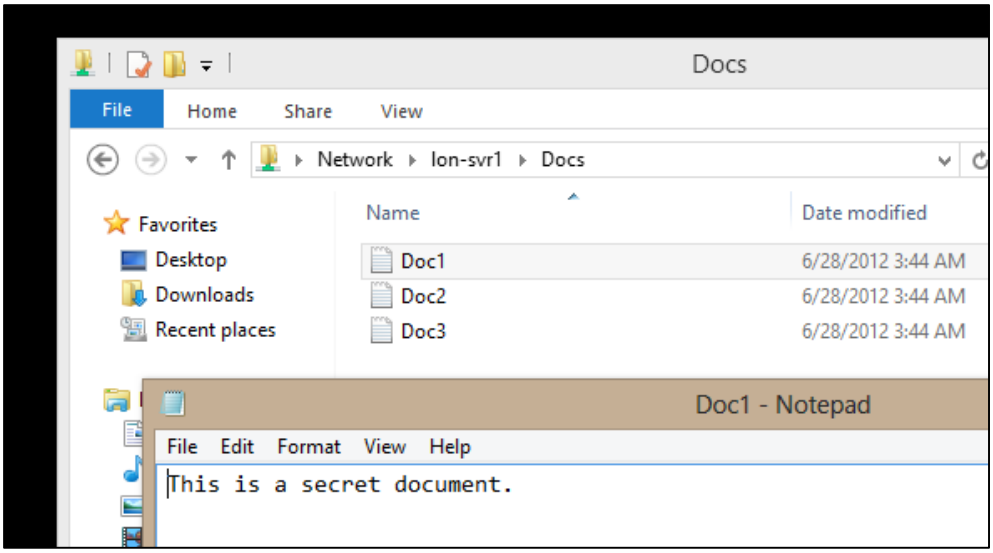


- Zugriff von Allie (Department = Research) auf \\lon-svr1\research (Client ist dabei egal)

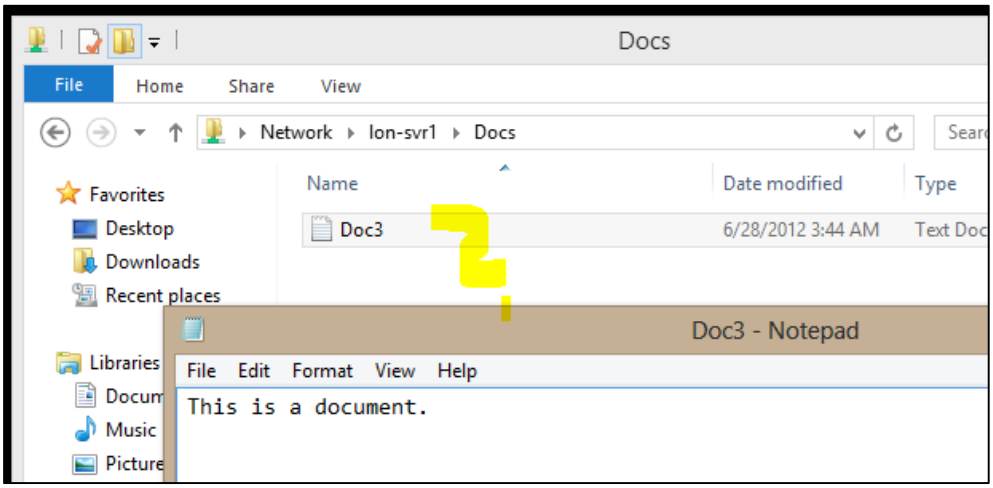


Test für die vertraulichen Dokumente

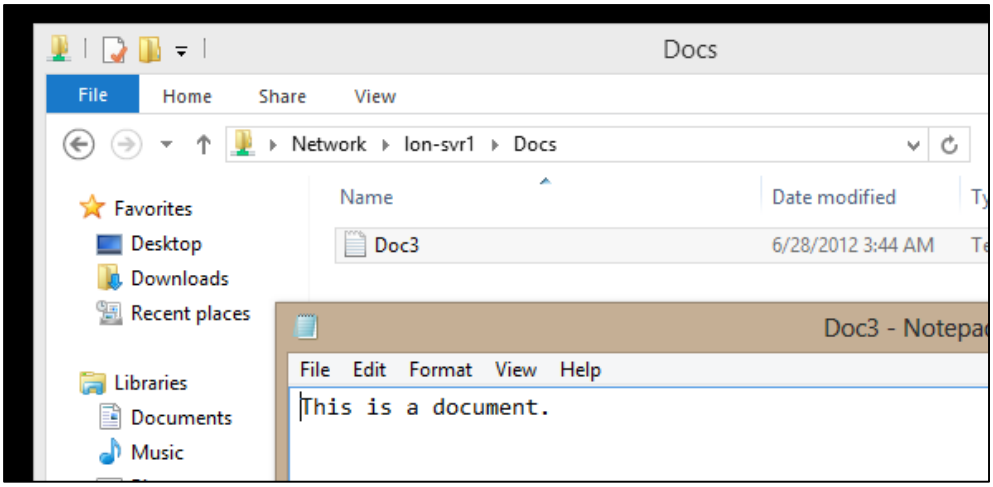
- Zugriff von Aiden (Department = Managers) auf \\lon-svr1\docs von lon-cl1 (in Gruppe WKS-Managers):



- Zugriff von Aiden (Department = Managers) auf \\lon-svr1\docs von lon-cl2 (kein Manager-PC):



- Zugriff von Allie (Department = Research) auf \\lon-svr1\docs von lon-cl1 (in Gruppe WKS-Managers):



- Zugriff von Allie (Department = Research) auf \\lon-svr1\docs von lon-cl2 (kein Manager-PC):