Inhalt

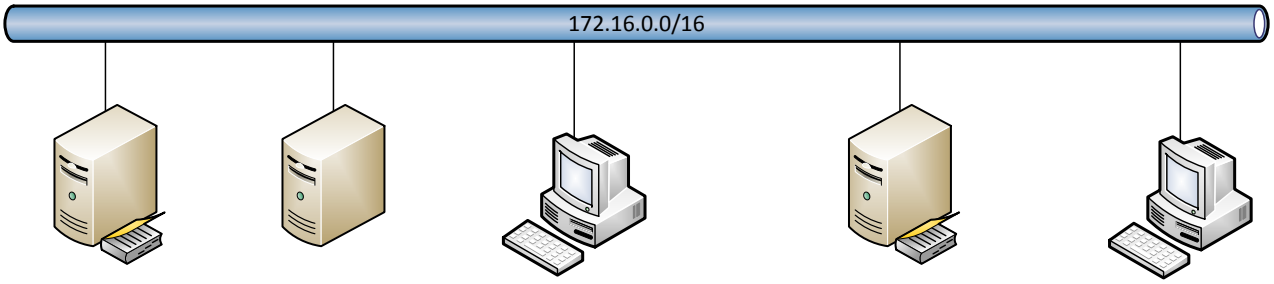
1) Szenario

Beschreibung

In der Firma Adatum soll ein AD-RMS installiert werden, damit die Mitarbeiter ihre Dokumente mit Office 2010 benutzerdefiniert intern schützen können.

Zusätzlich soll ein AD-RMS-Vertrauen zur Gesamtstruktur der Firma Treyresearch hergestellt werden, damit deren Benutzer Dokumente aus Adatum verwenden können.

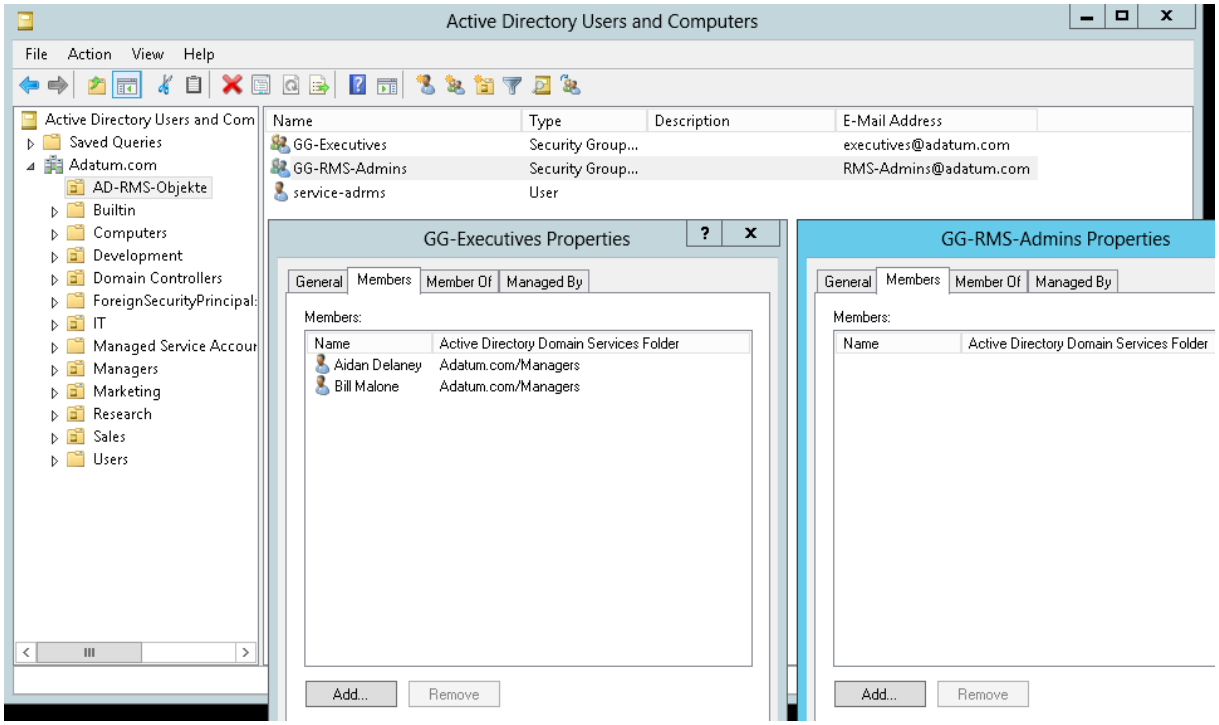
Netzwerkplan:



2) Vorbereitungen im Active Directory und DNS

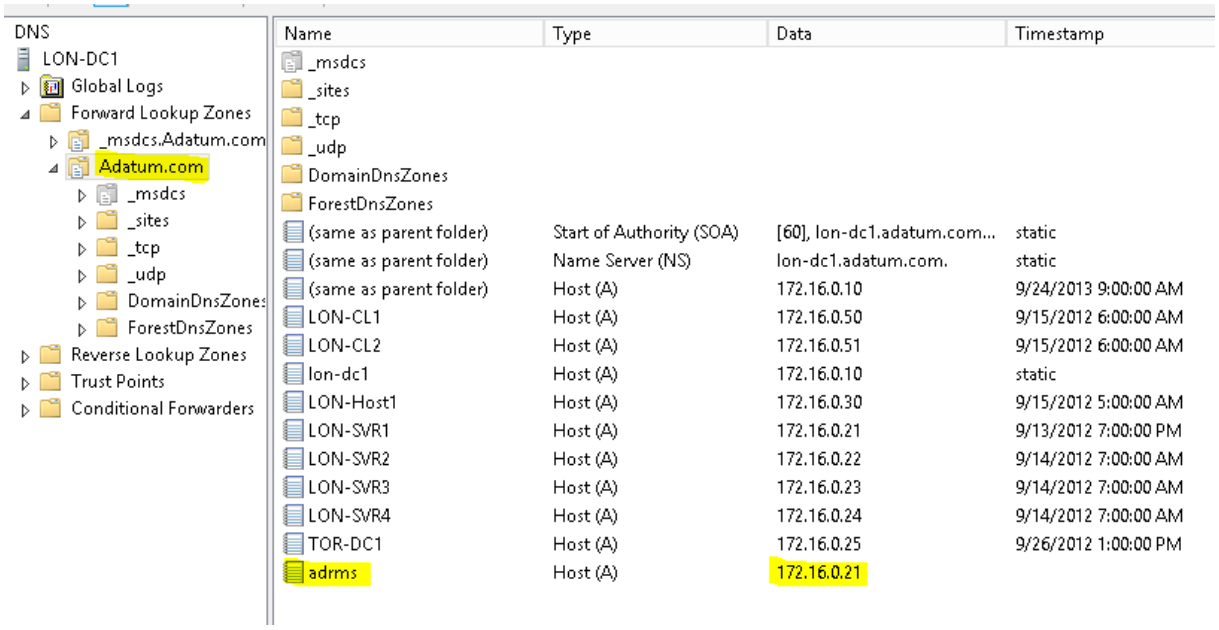
Vorbereitung im Active Directory

- Baue neue Organisationseinheit (zur Übersichtlichkeit)
- Baue für den Service des RMS-Servers einen neuen AD-Benutzer adatum\service-rms. Dies muss ein normaler Domänenbenutzer ohne besondere Rechte sein.
- Baue 2 neue AD-Gruppen mit konfigurierter Mailadresse:



Konfiguration im DNS

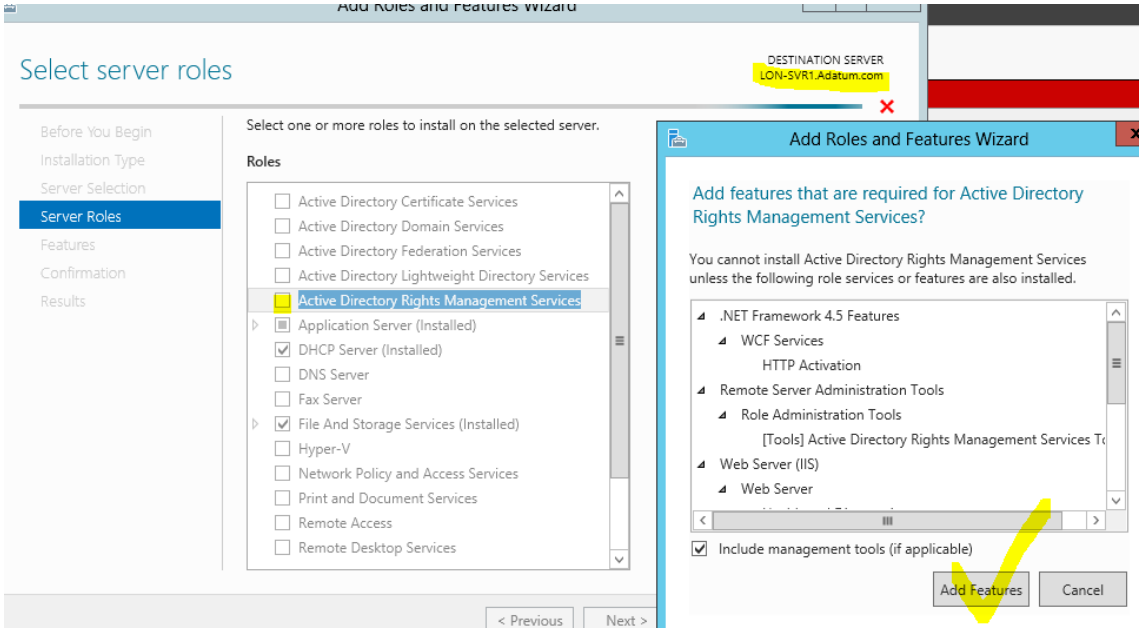
- Erstelle einen Host-A-Record auf den neuen AD-RMS-Server:

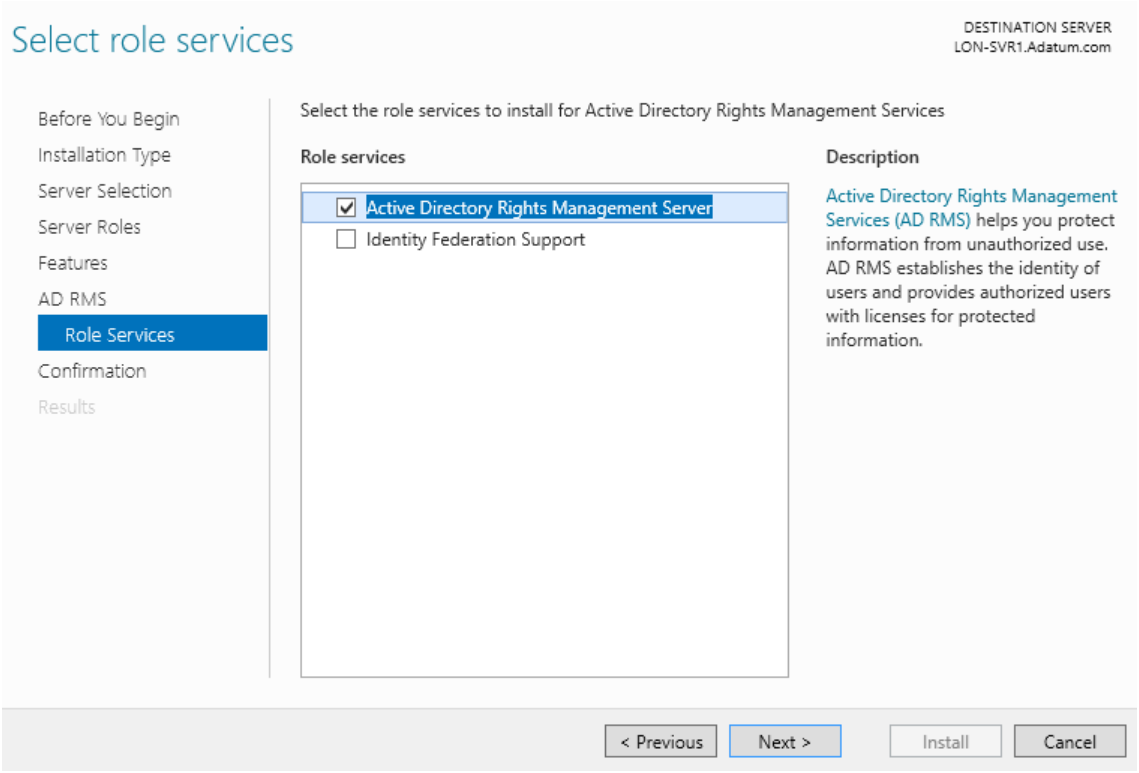


3) Installation und Konfiguration des AD RMS

Installation der Rolle

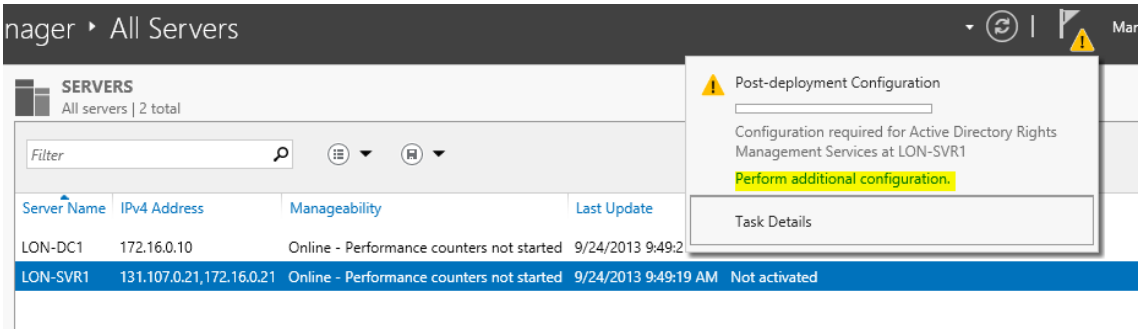
- Installiere über dem Servermanager von LON-DC1 auf LON-SVR1 die Rolle AD-RMS:



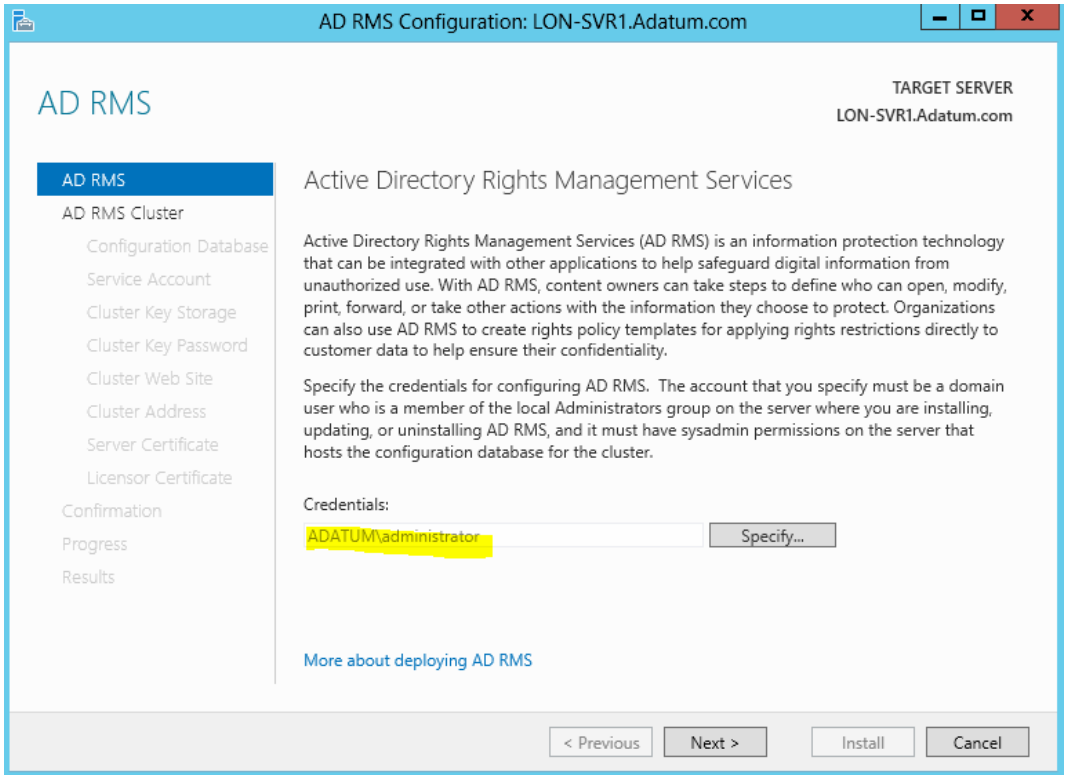


Konfiguration der Rolle

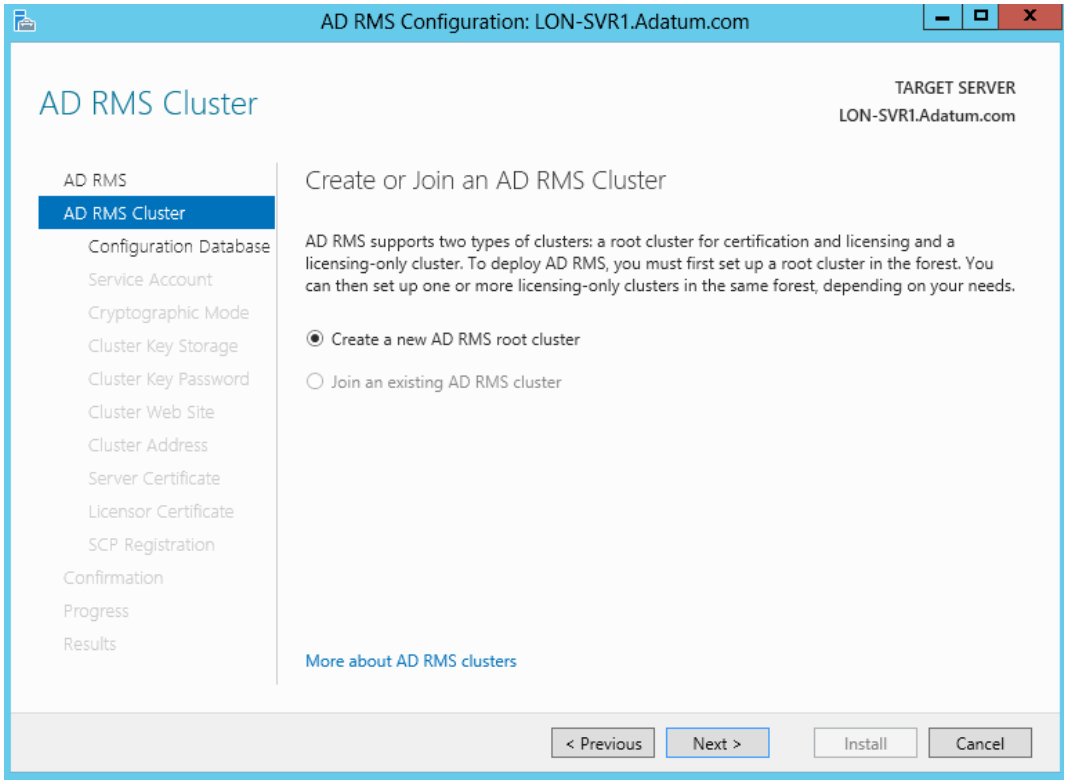
- Wähle im Servermanager den Konfigurationsassistenten aus:



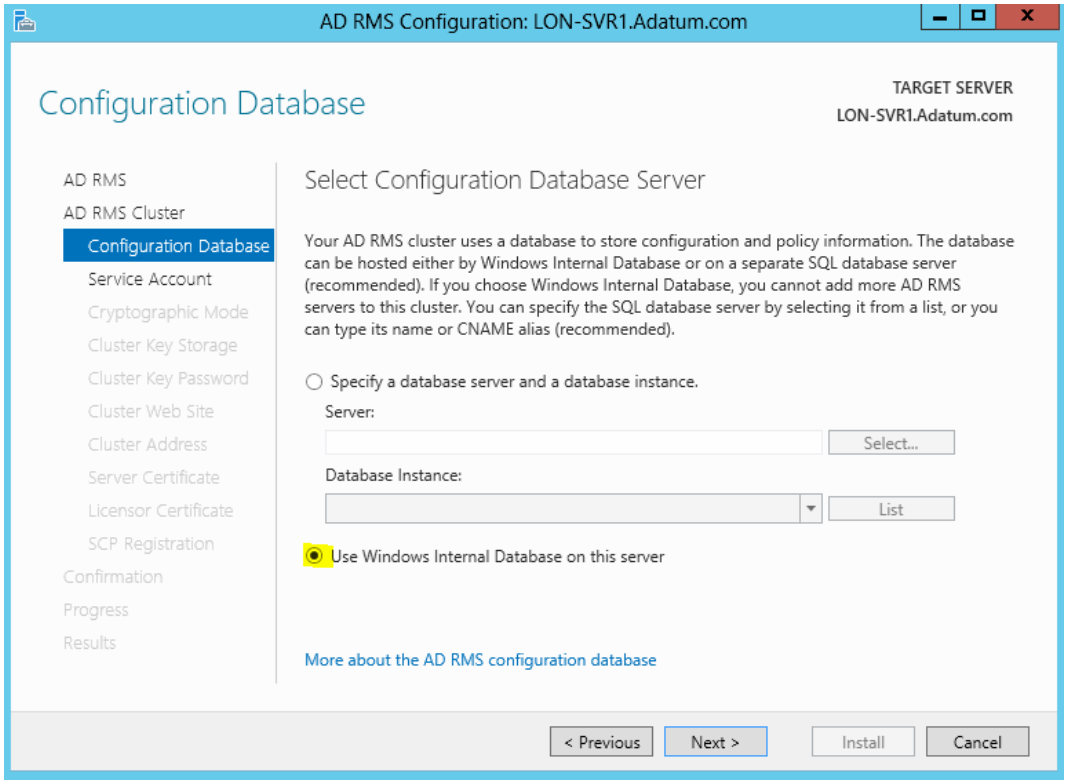
- Anmeldedaten angeben:



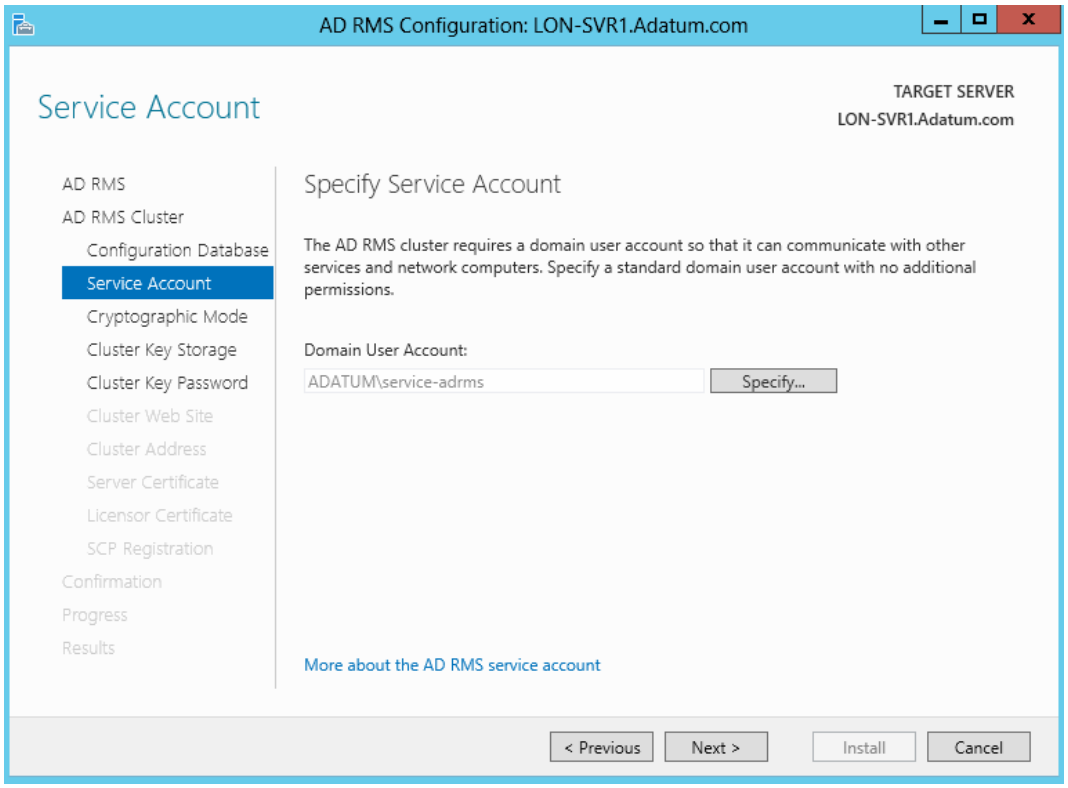
- Erstelle neuen AD-RMS-Cluster:



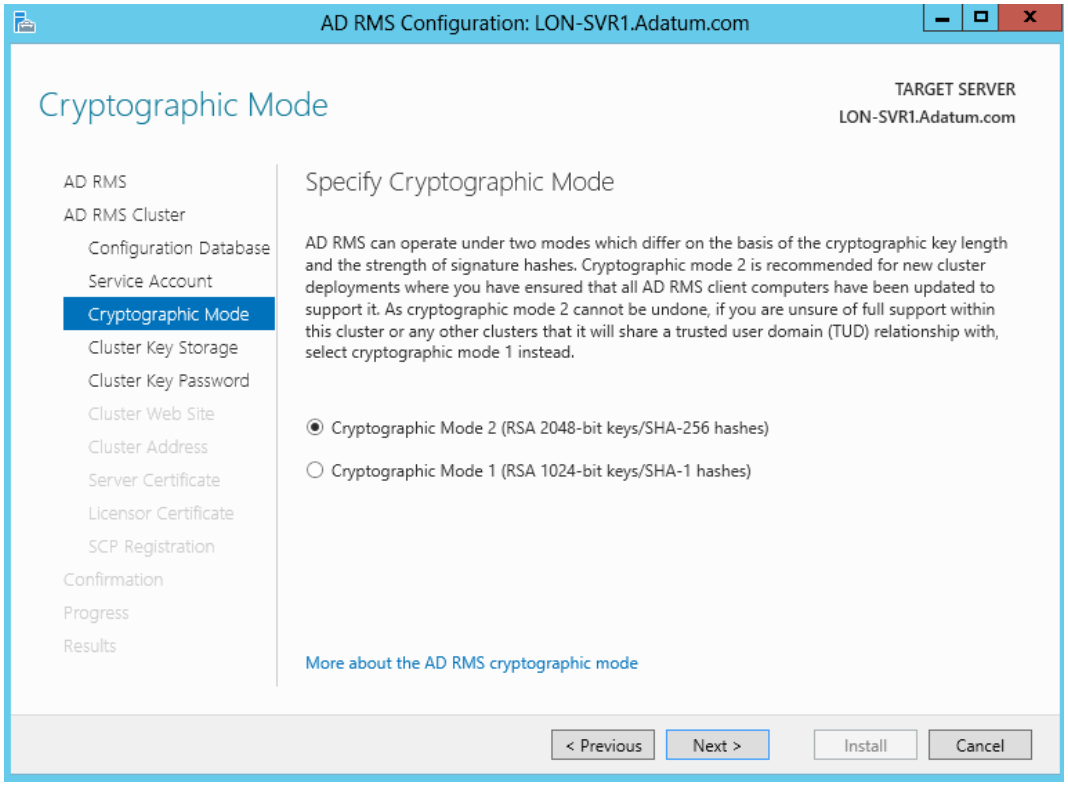
- Erstelle neue Windows-Internal-Database (besser wäre für die Verfügbarkeit und auch für die Skalierbarkeit der RMS-Server eine SQL-Instanz. Diese sollte auch selbst verfügbar sein (SQL-Cluster/AlwaysOn):



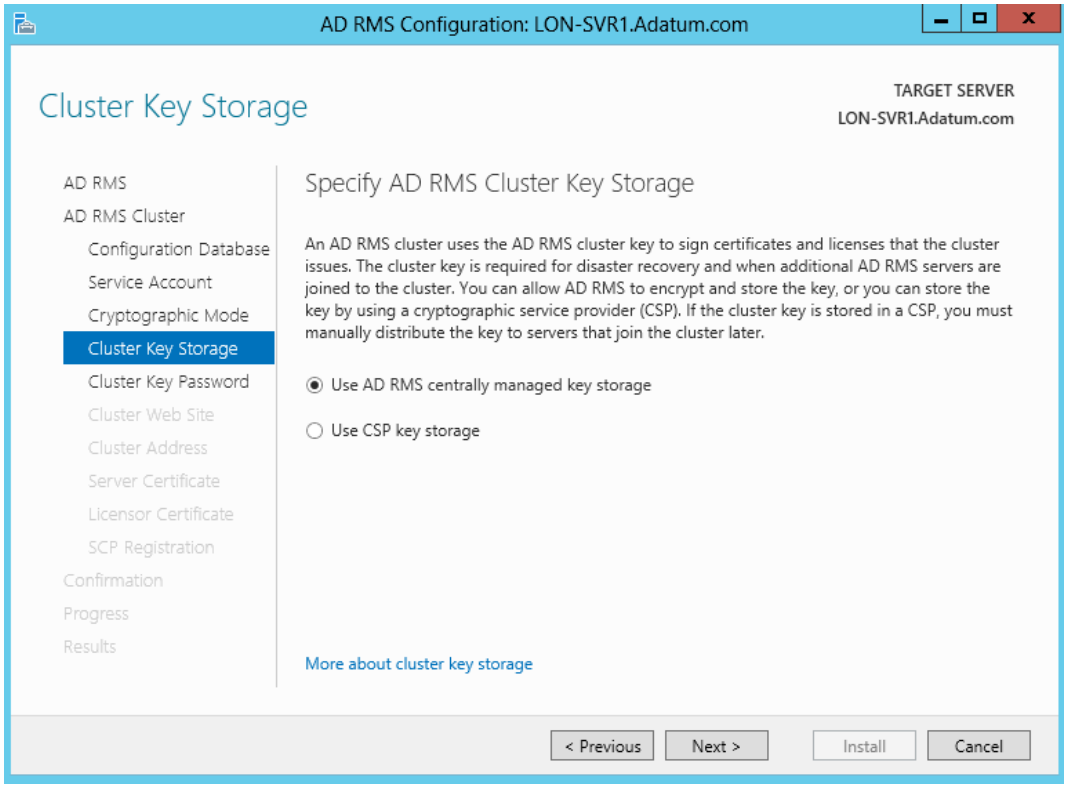
- Übergib den Service-Benutzer (Standard-AD-Benutzer ohne zusätzliche Rechte!):



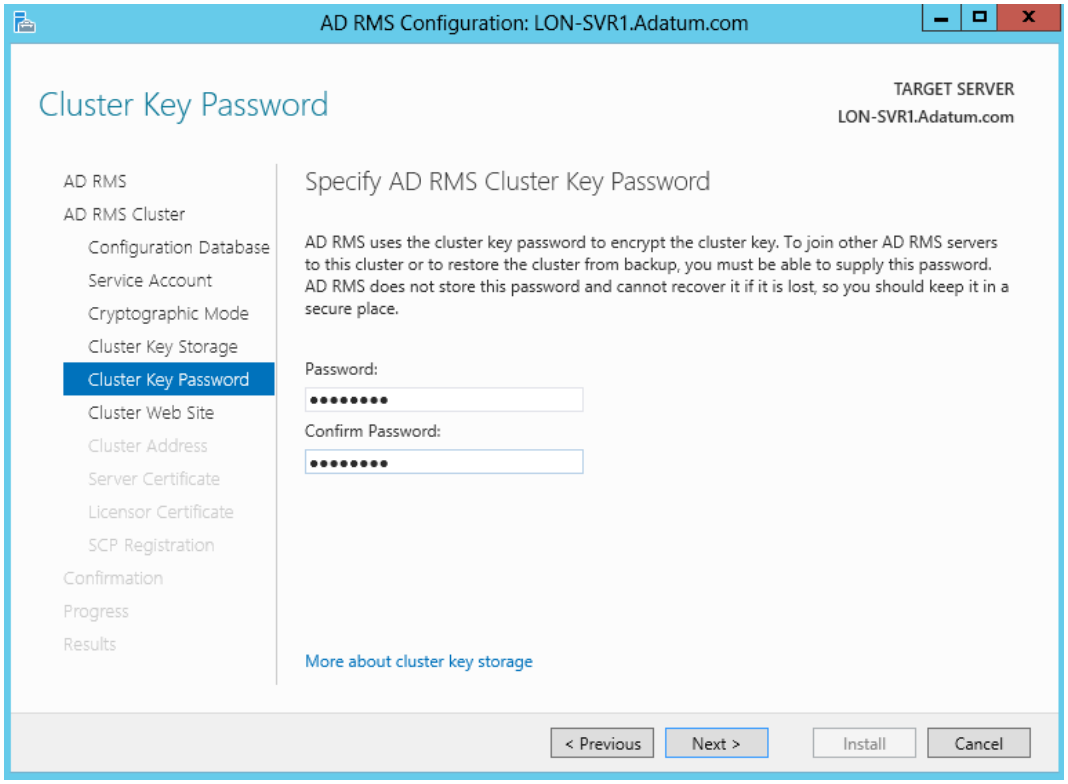
- Wähle den Kryprografiemodus aus:



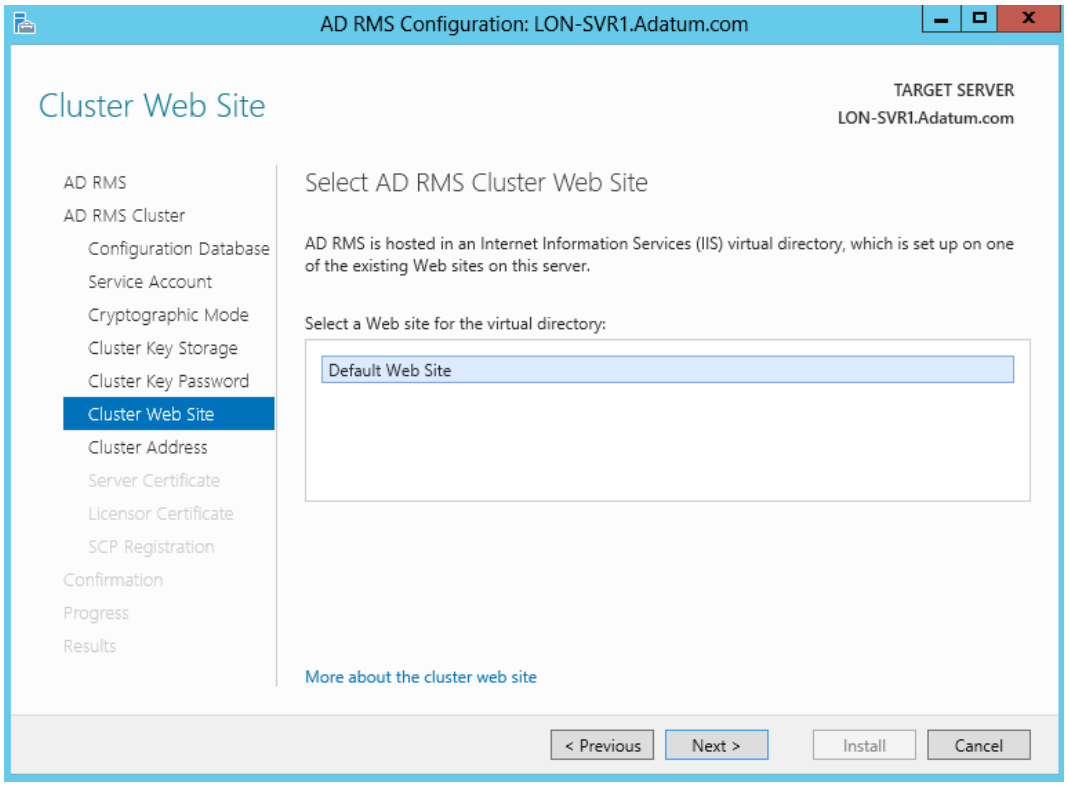
- Wähle Schlüsselspeicherlayout:



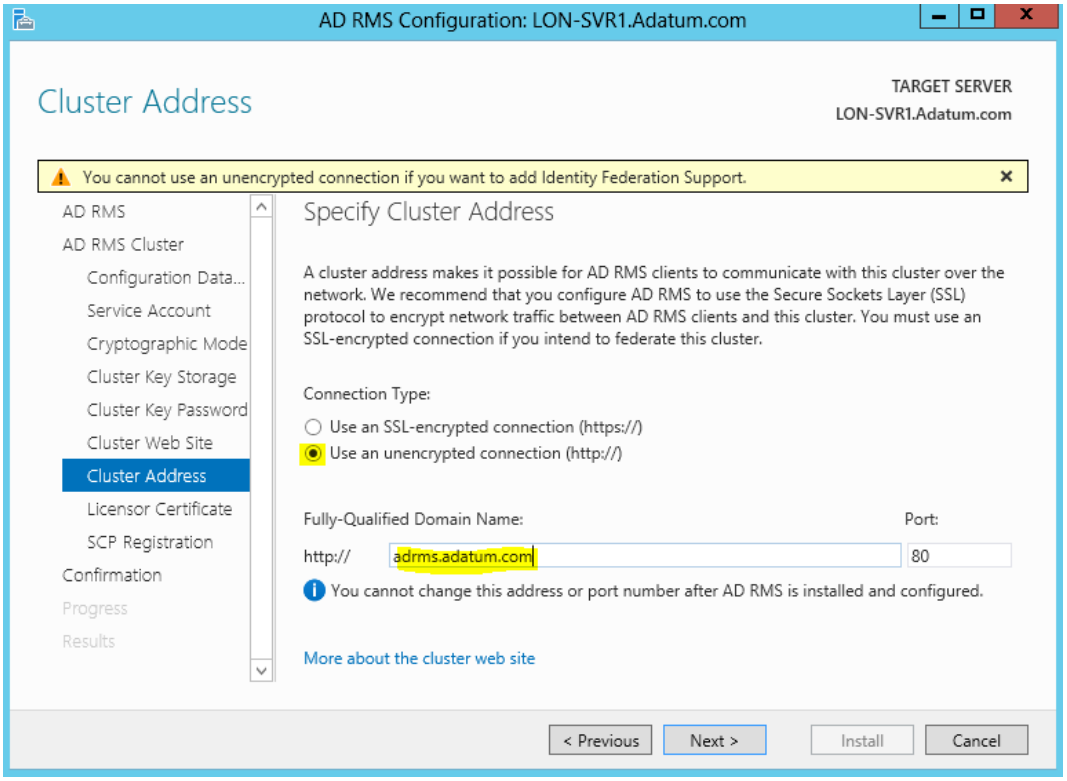
- Angabe des symmetrischen Schlüssels, der den Schlüsselspeicher schützt:



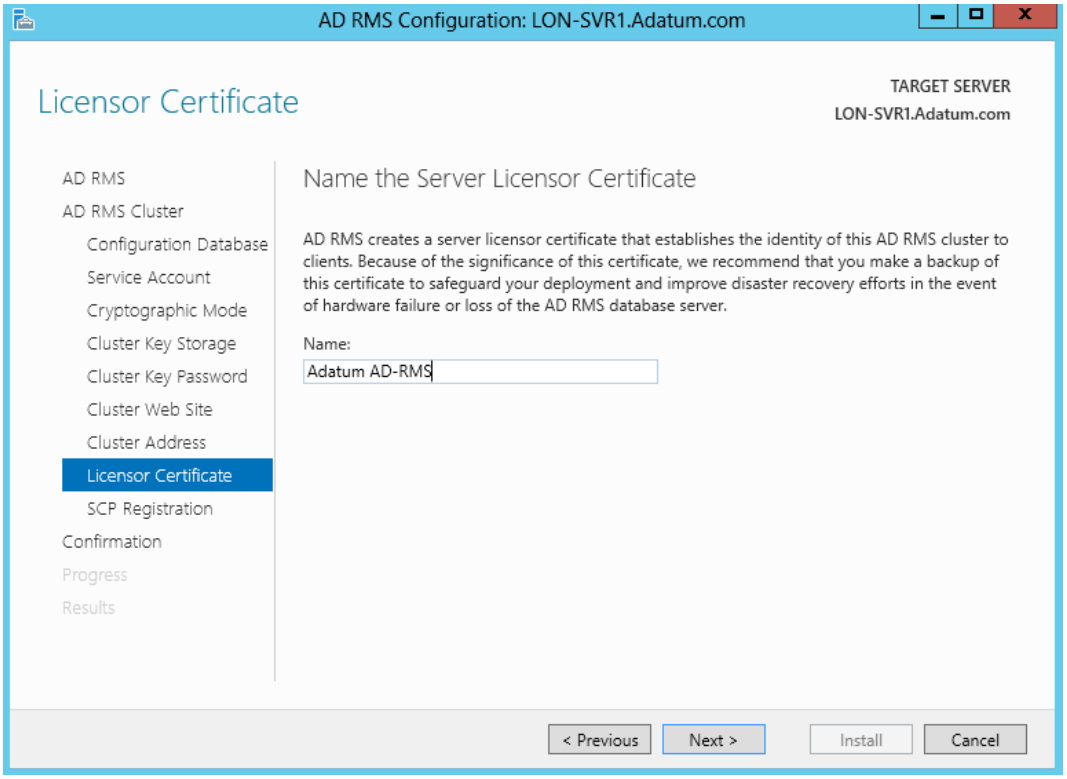
- Angabe der Cluster-Website:



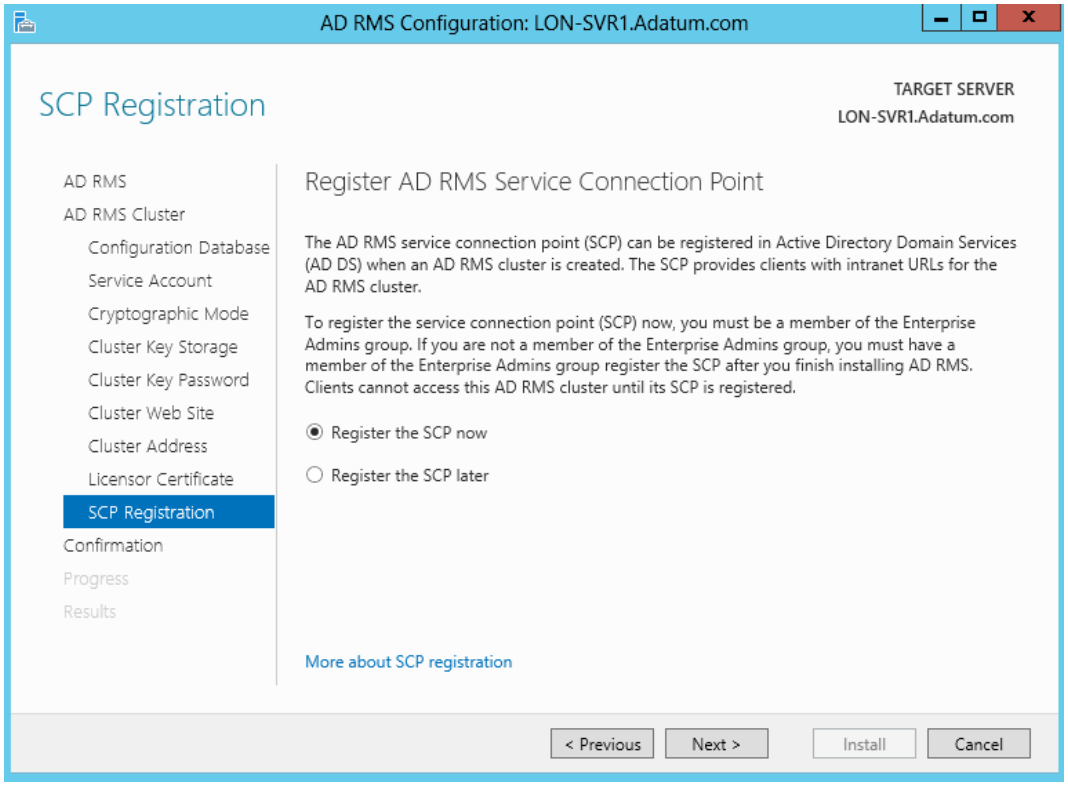
- Definiere den Zugriff auf die Clusterwebsite:



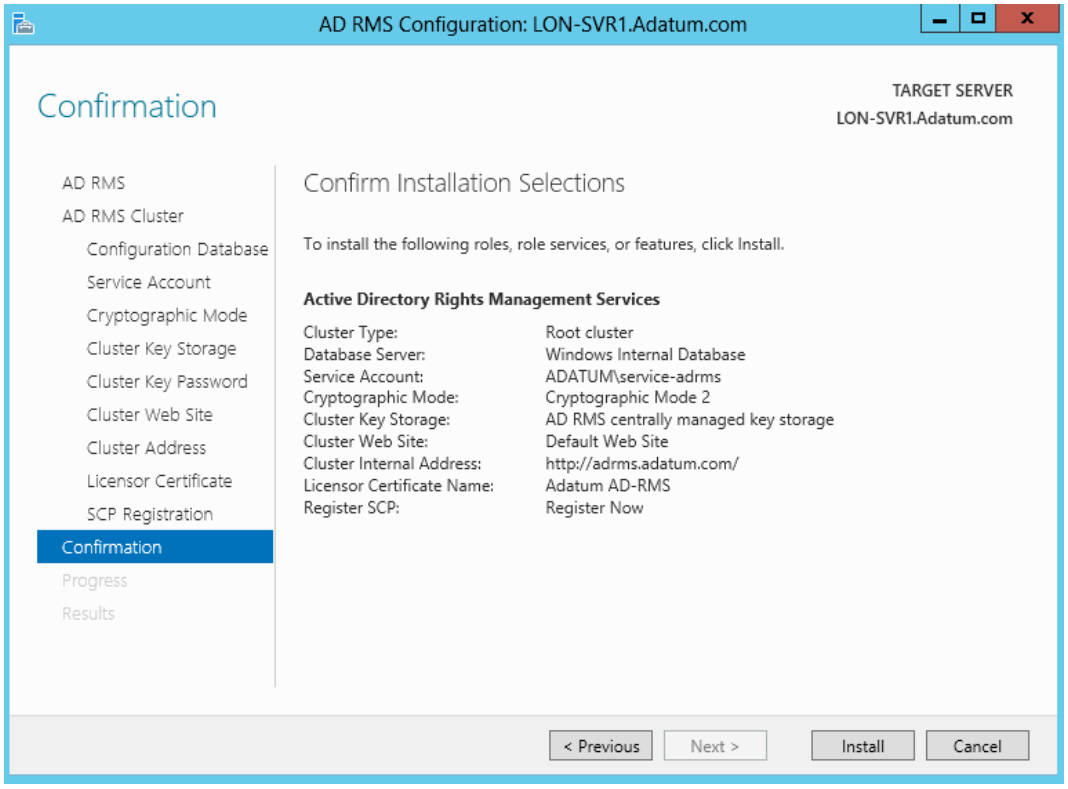
- Definiere den Anzeigenamen des Stammzertifikates:



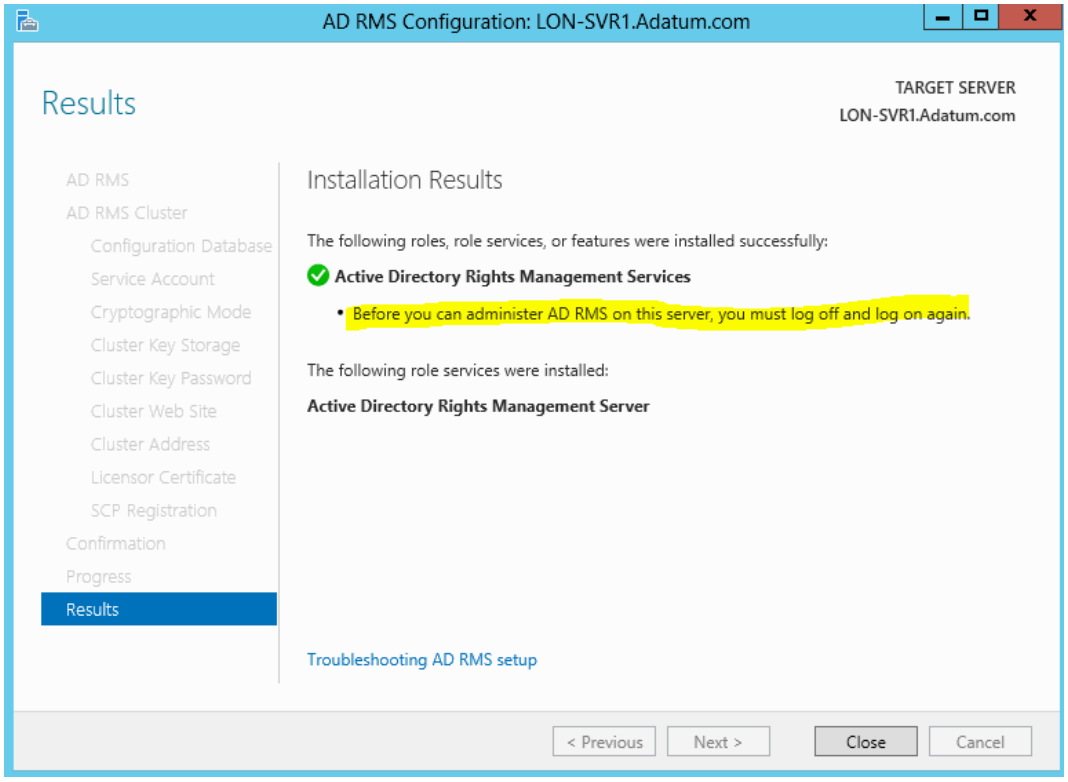
- Die Konfiguration des Service-Connection-Points kann vom Assistenten vorgenommen werden:



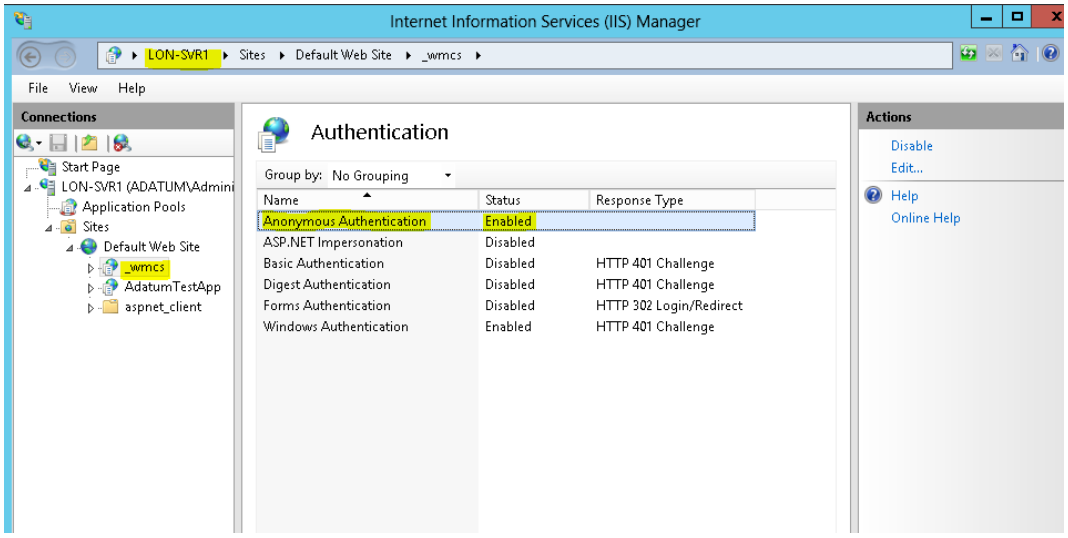
- Start der Konfiguration:



- Abschluss der Konfiguration:



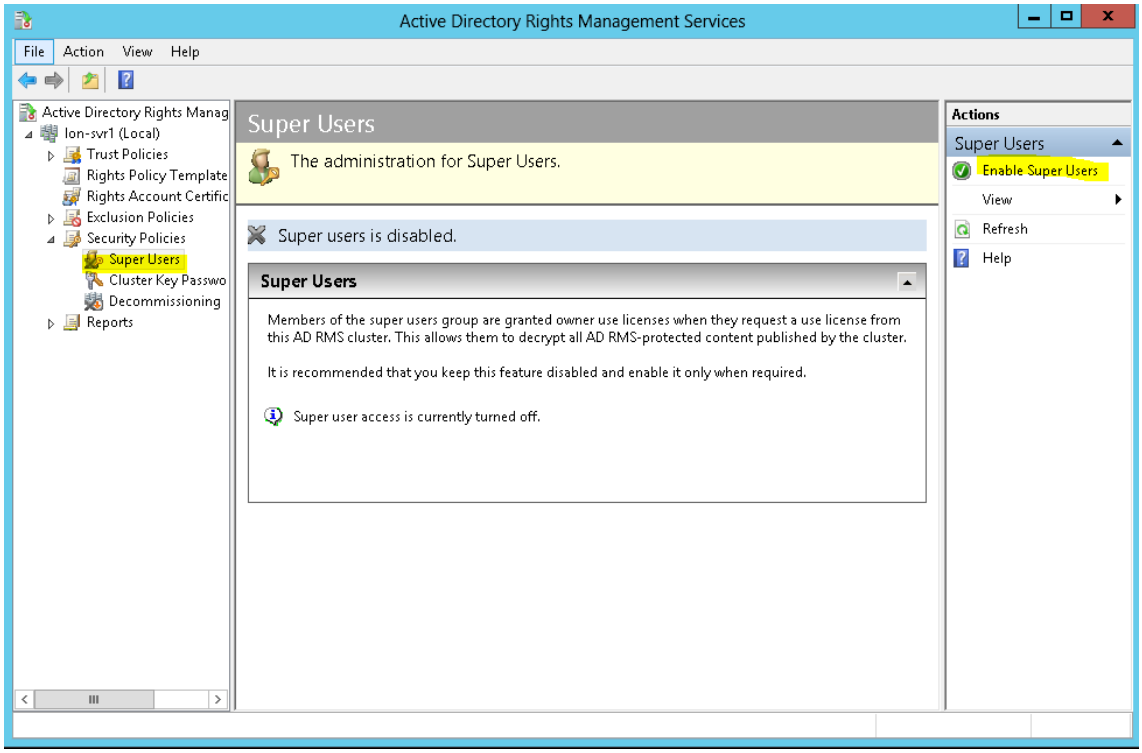
- Konfiguriere den anonymen Zugriff auf das Verzeichnis _wmcs der Cluster-Website im IIS auf LON-SVR1:



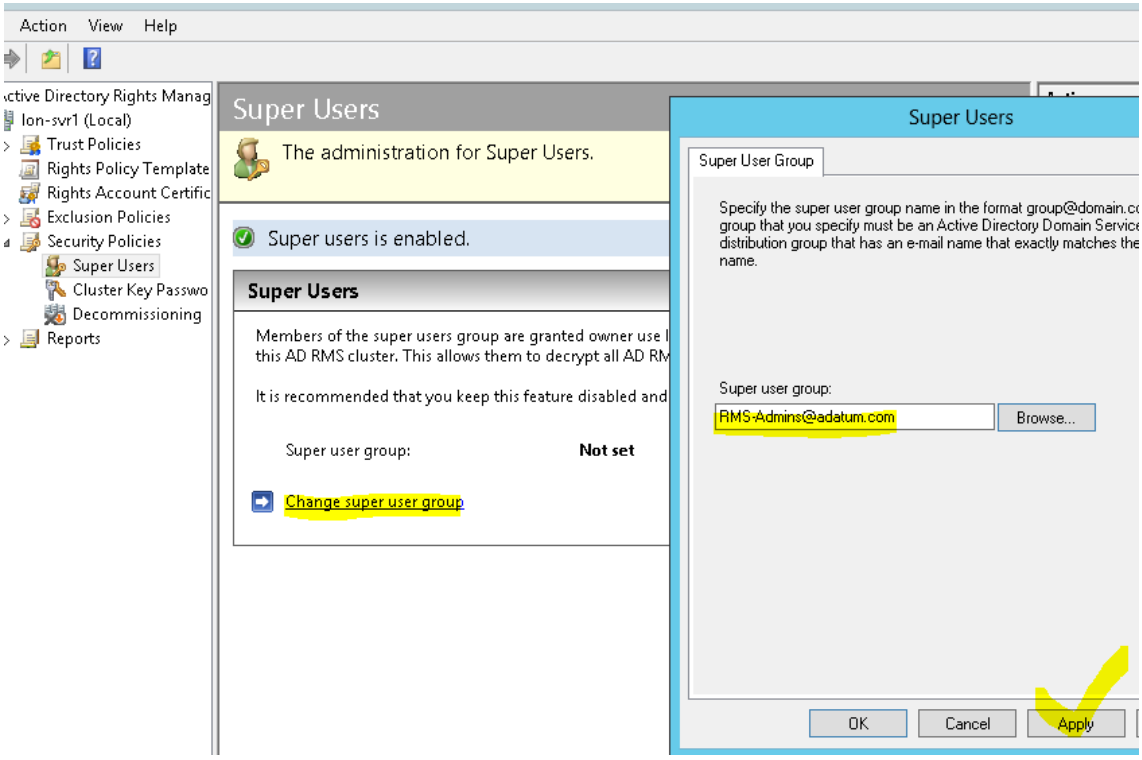
- Abmelden und wieder als Administrator anmelden.

Konfiguration der Administratorengruppe für RMS

- Starte AD-RMS-Managementkonsole
- Ändere die Administratorenkonfiguration:



- Konfiguriere die Administratorengruppe:



4) Konfiguration der RMS-Vorlagen

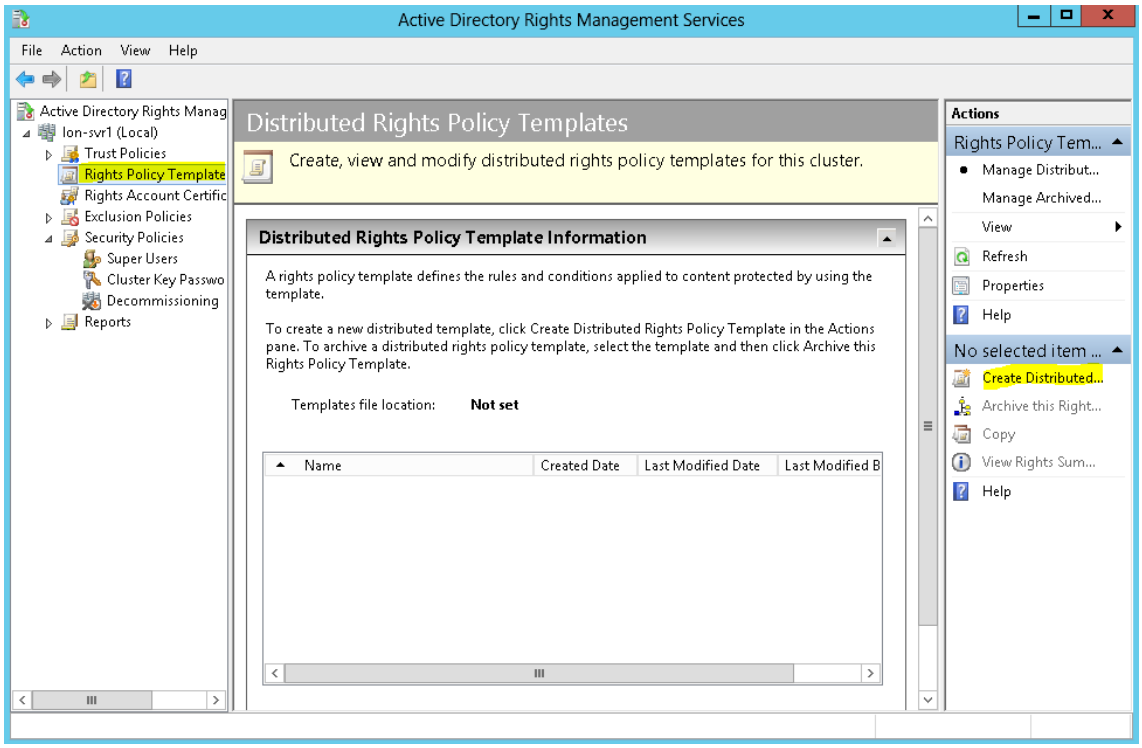
Freigaben für AD-RMS

- Erstelle Freigaben auf LON-SVR1:

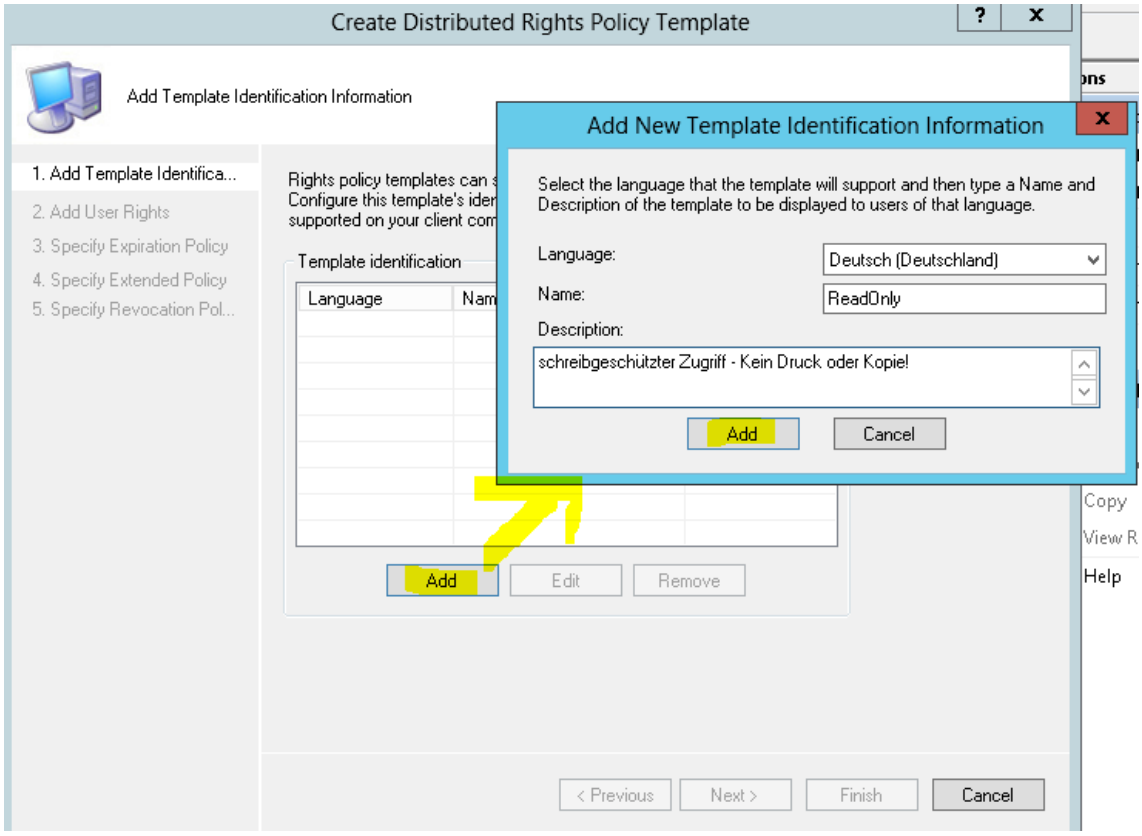
```
New-Item C:\RMS-Templates -ItemType Directory
New-SmbShare -Name RMS-Templates -Path C:\RMS-Templates -FullAccess adatum\service-adrms

New-Item C:\Dokumente -ItemType Directory
New-SmbShare -Name Dokumente -Path C:\Dokumente -FullAccess everyone

New-Item C:\Export -ItemType Directory
New-SmbShare -Name Export -Path C:\Export -FullAccess everyone
```

Konfiguration einer neuen Vorlage für die Benutzerrechterichtlinien

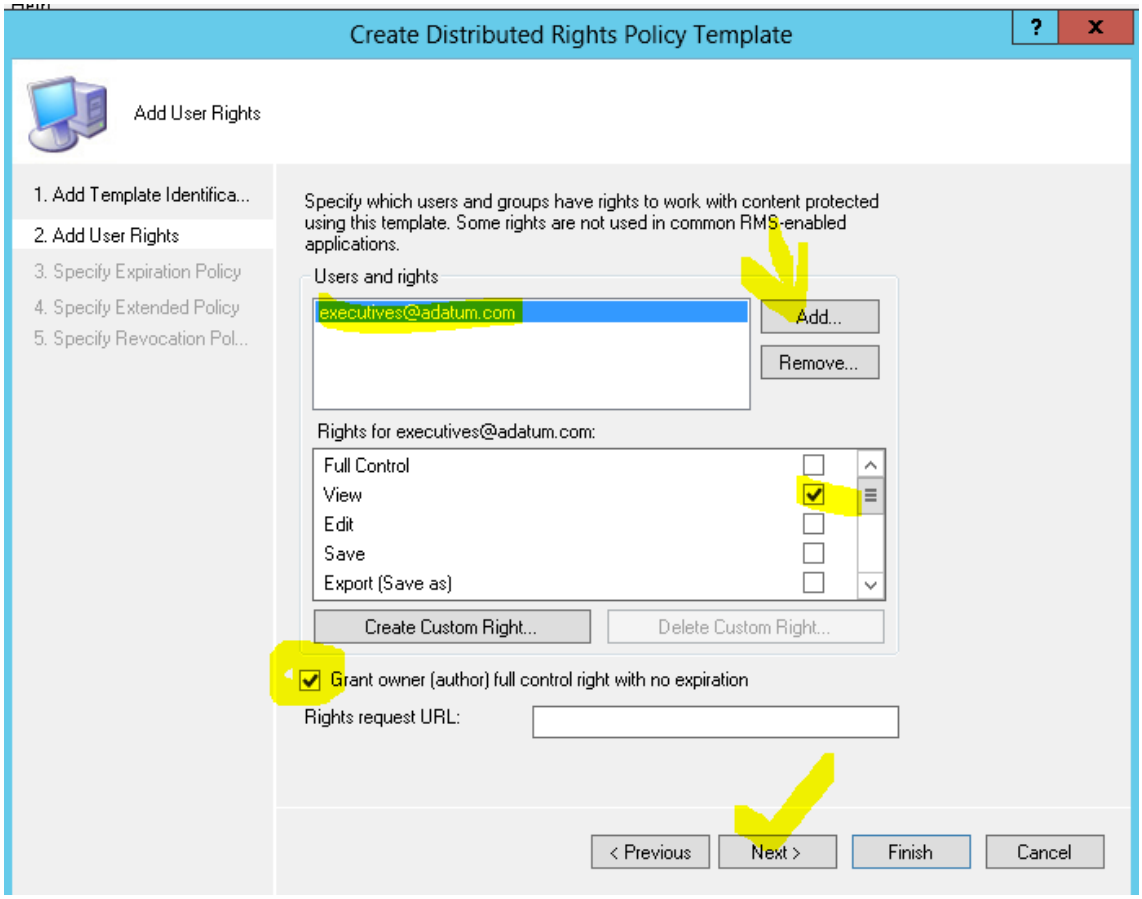
- Erstelle eine neue Vorlage in der Management-Konsole:



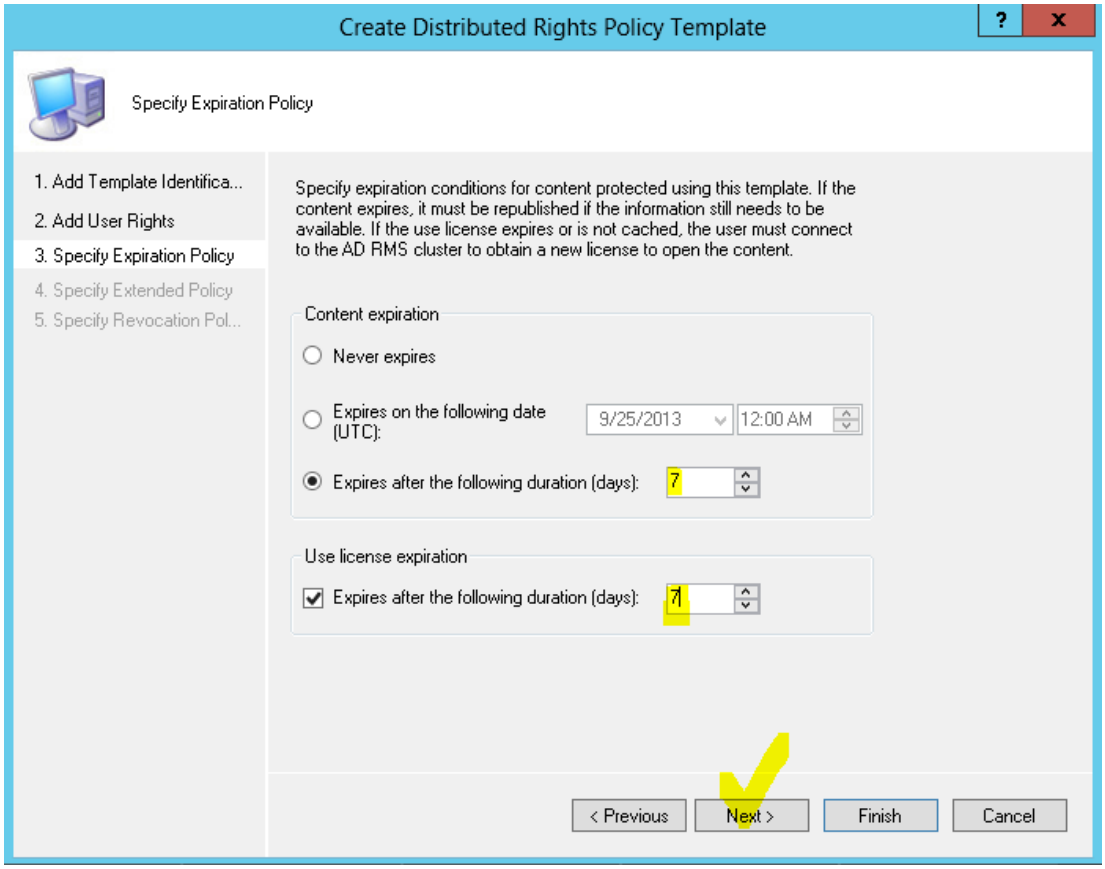
- Definiere neue Identifizierungsinformation:



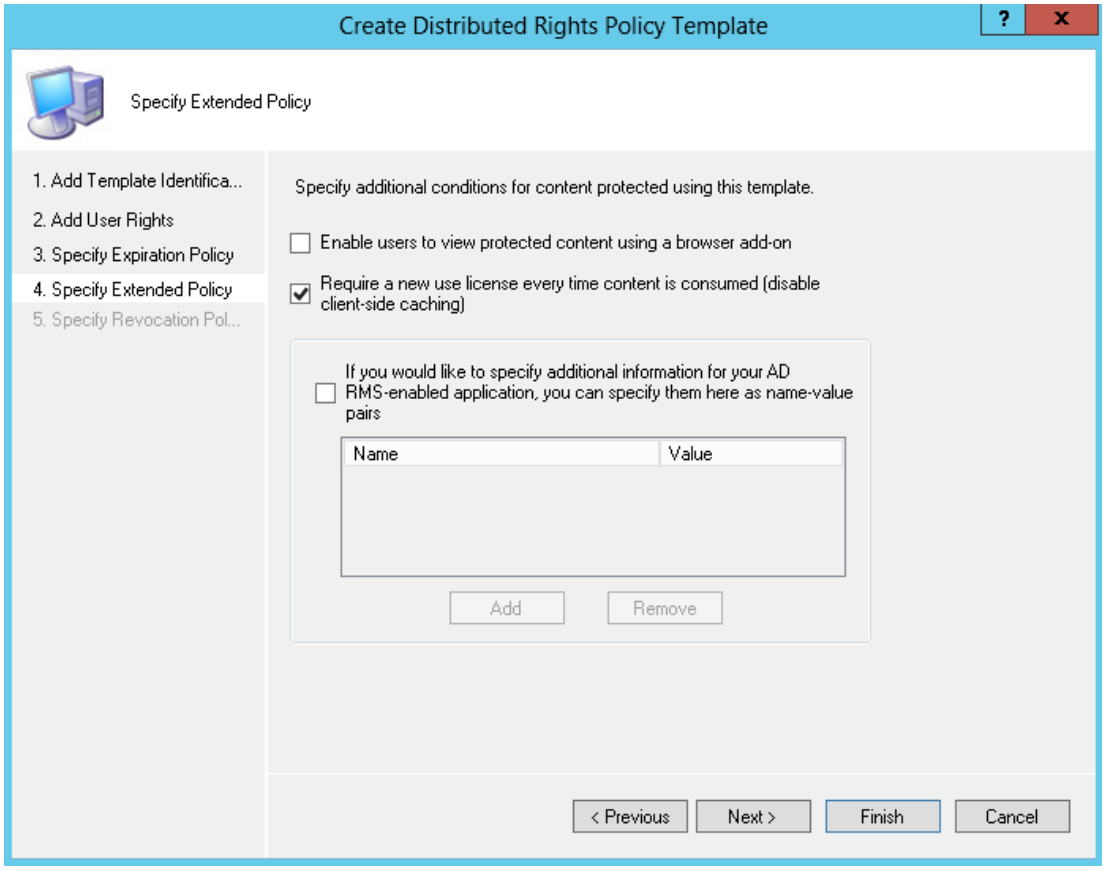
- Wähle die Rechte zu den Identitäten aus:



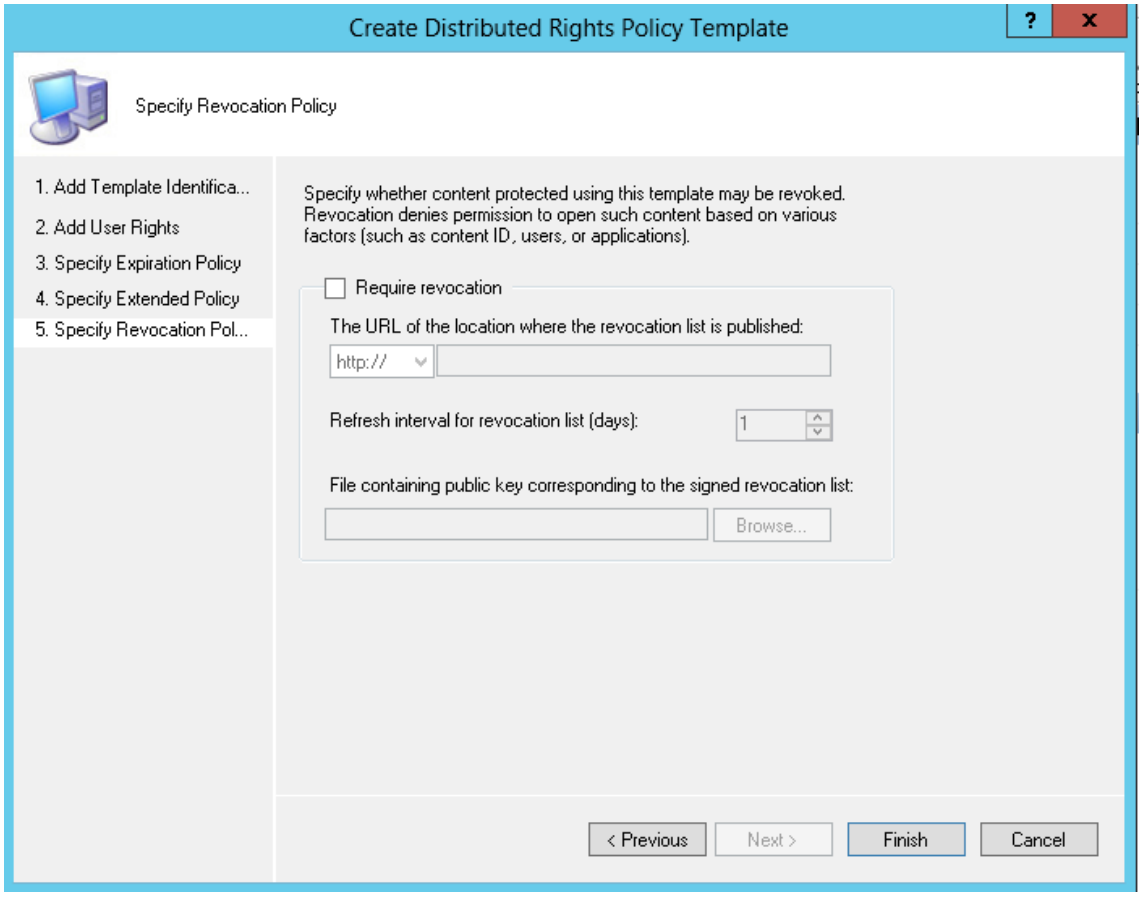
- Konfiguriere den Ablauf der Zugriffslizenz und den Inhaltsablauf:



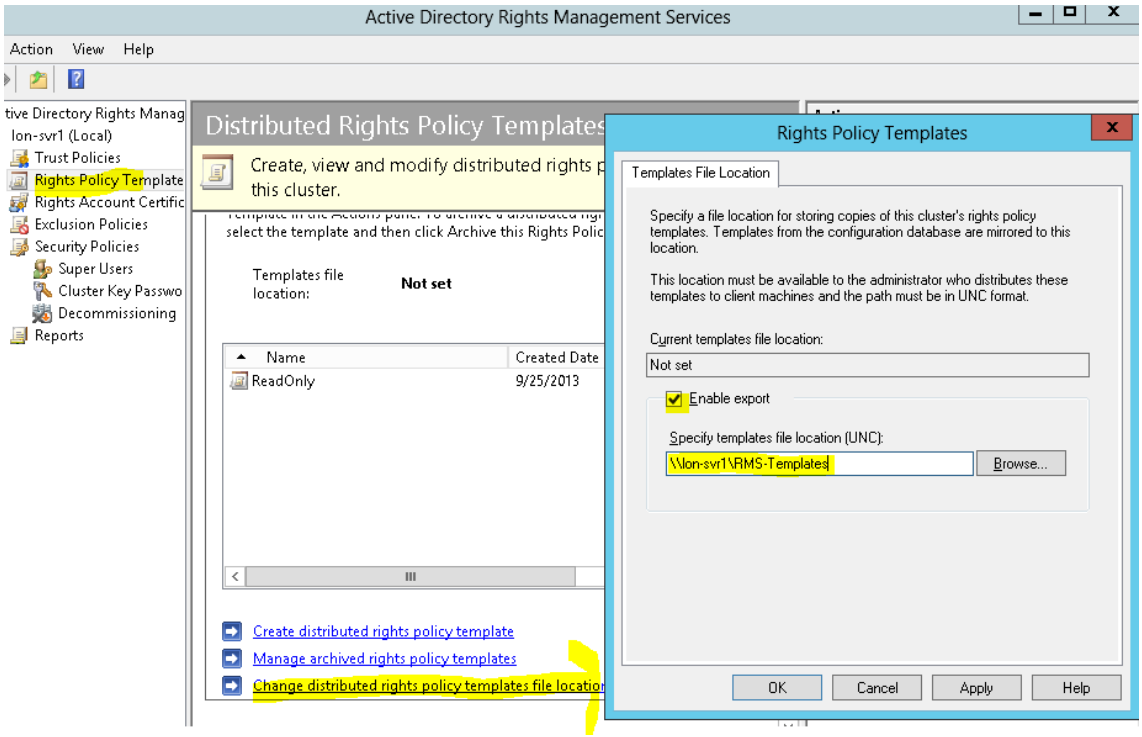
- Erzwinge das Abrufen von Lizenzinformationen bei jeder Verwendung:



- Konfiguration der Sperrliste für ungültige Zertifikate (durch die Begrenzung auf 7 Tage wird diese hier nicht benötigt):

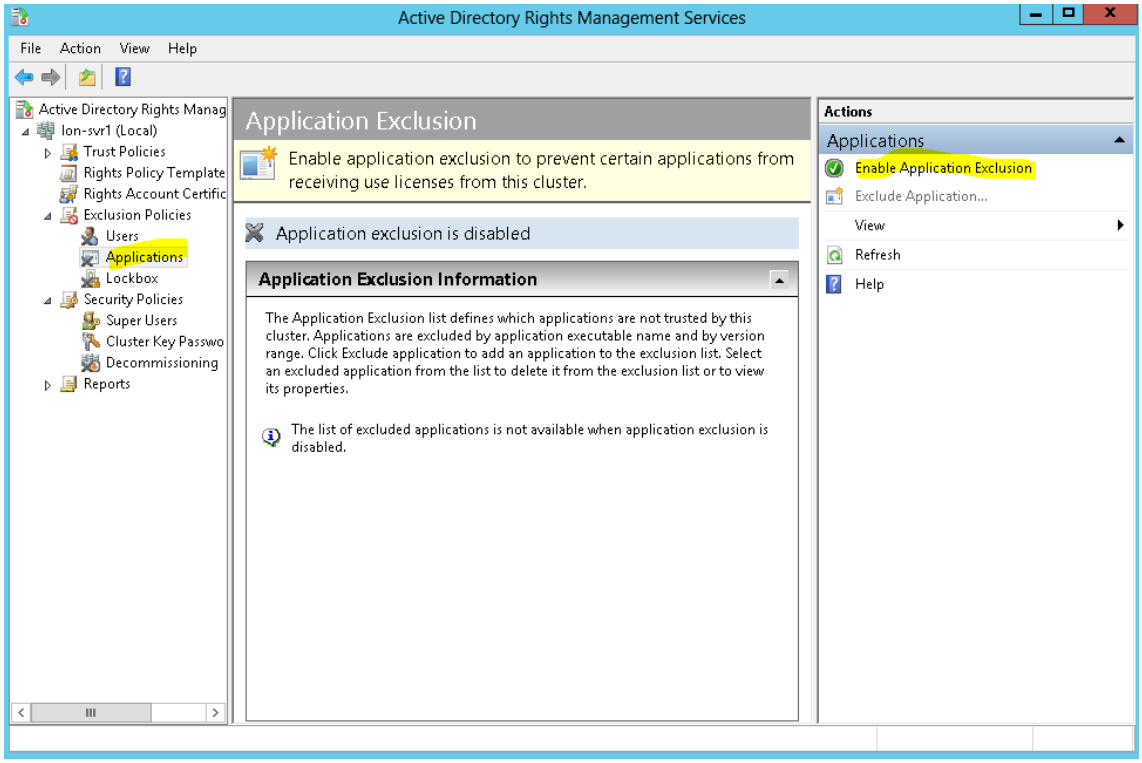


- Veröffentlichung der Vorlage in der neuen Freigabe:

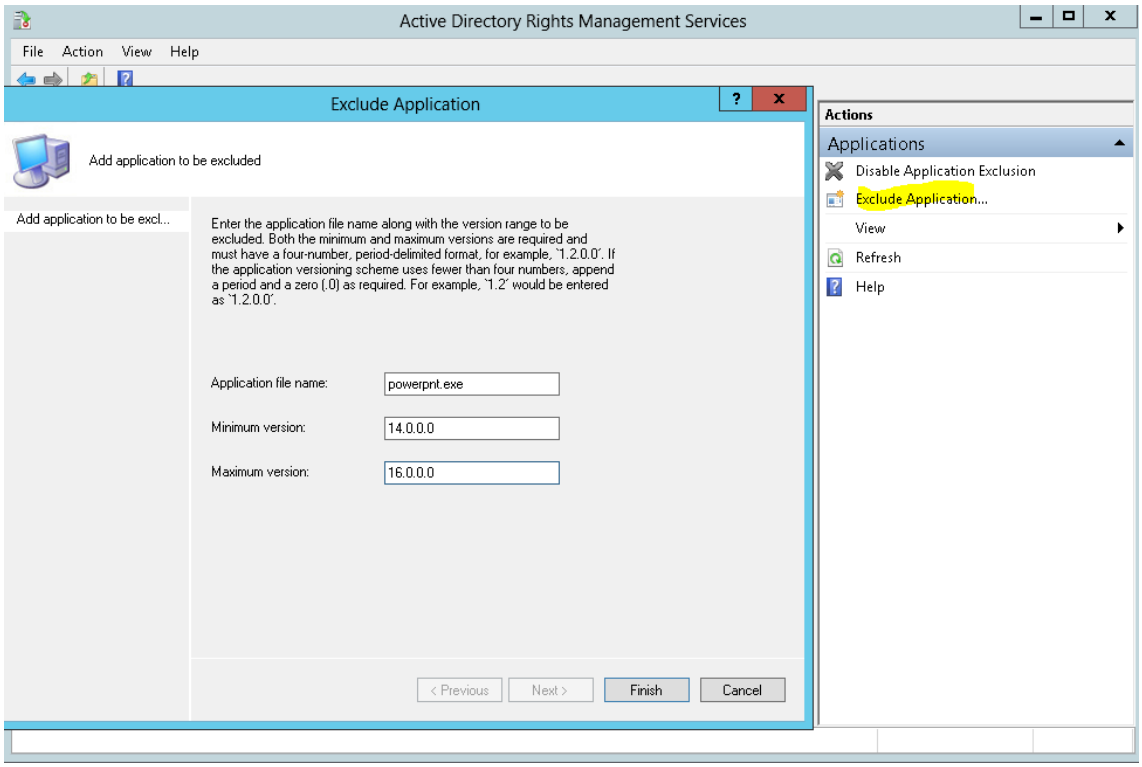


Konfiguration einer Ausschlussrichtlinie

- Aktivierung des Anwendungsausschlusses:



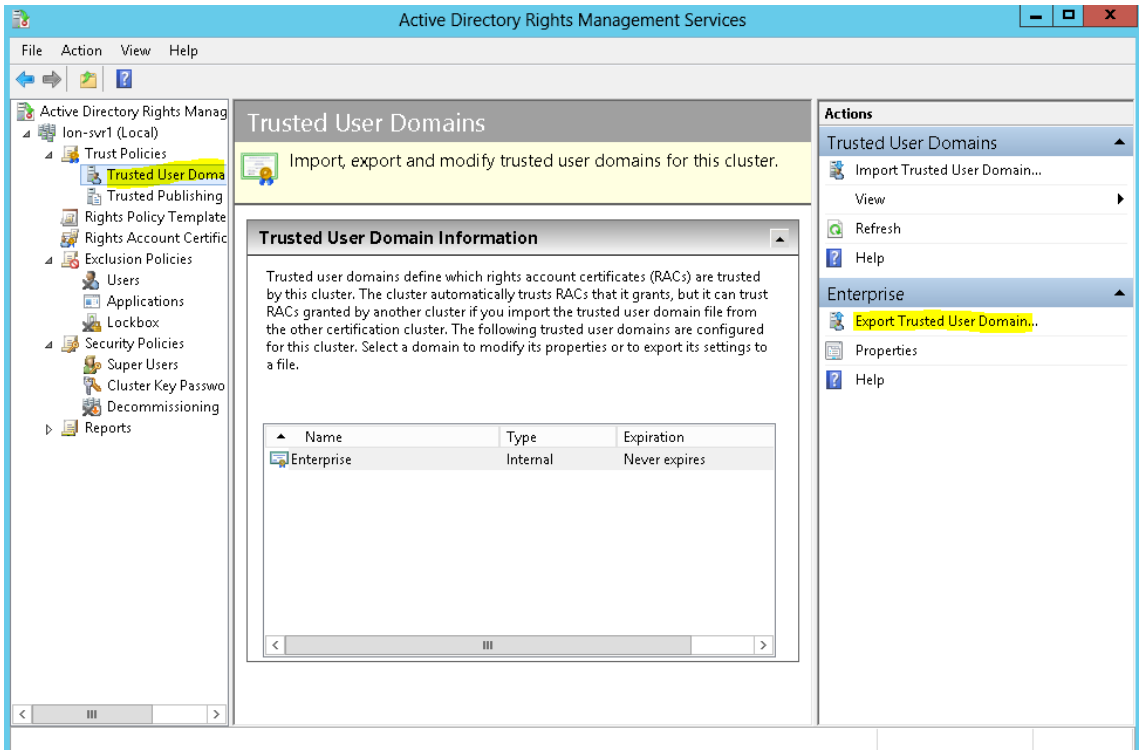
- Nehme Powerpoint aus RMS raus:

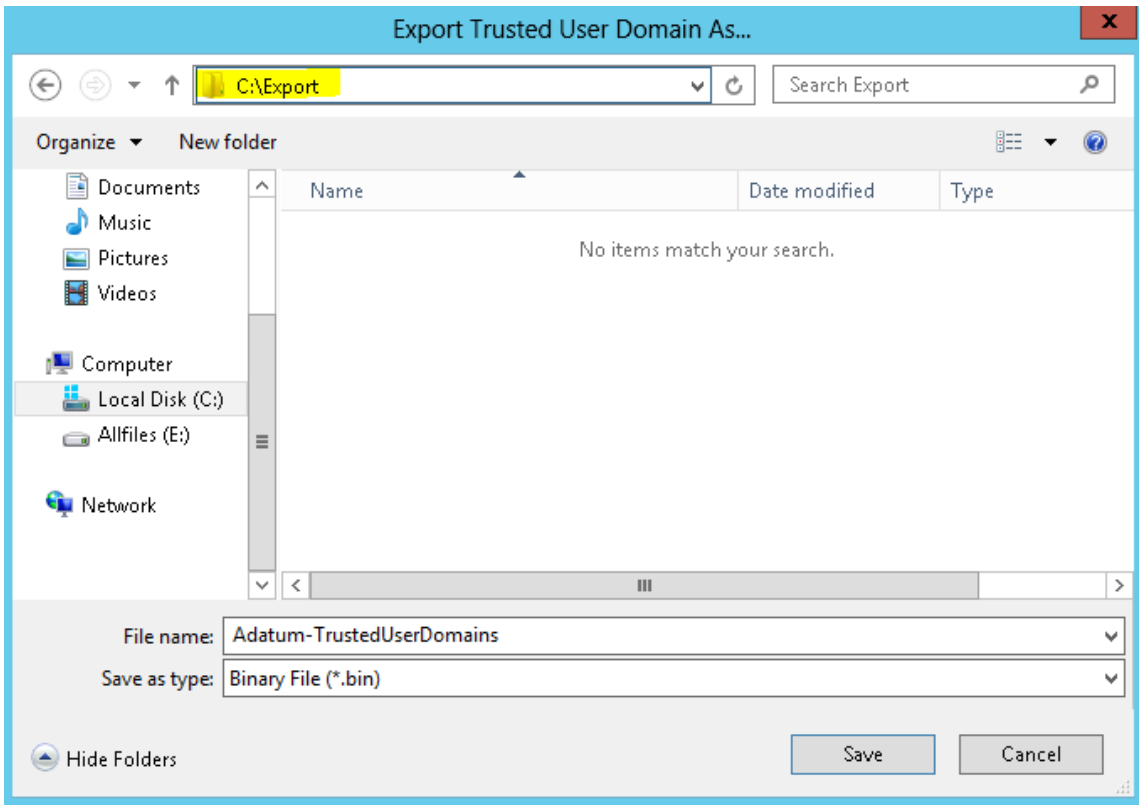


5) Implementation der Vertrauensrichtlinien

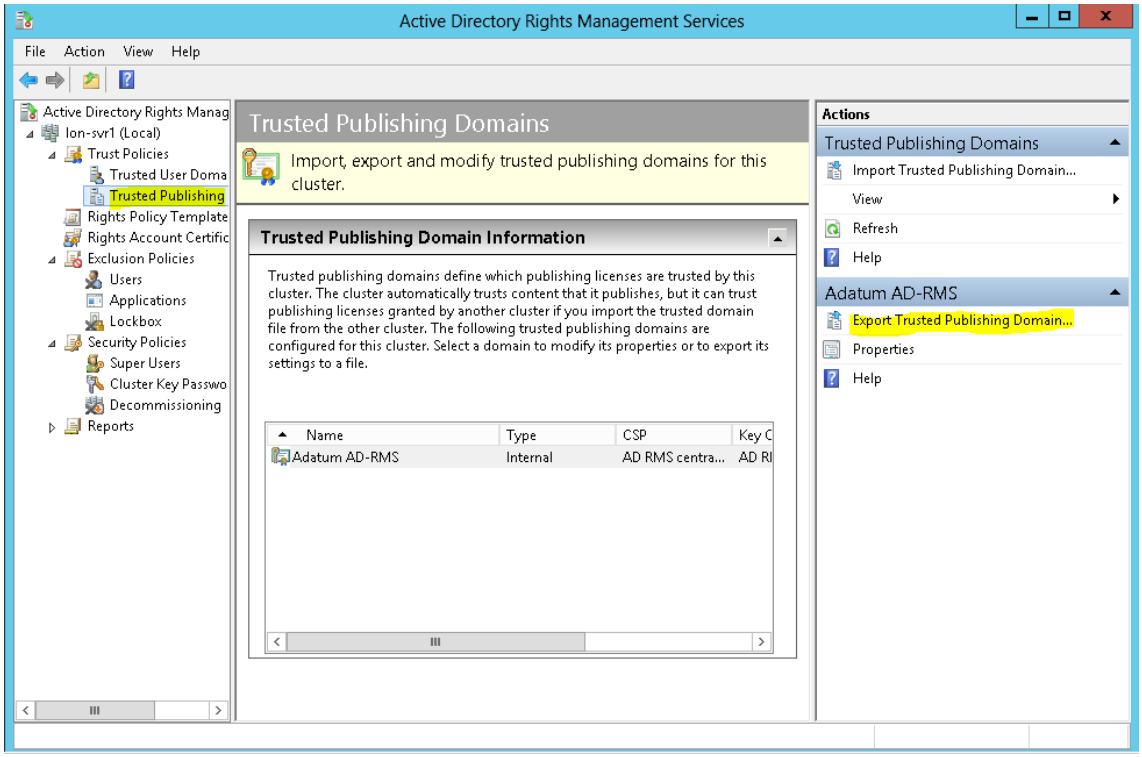
Exportieren der Vertrauensrichtlinie

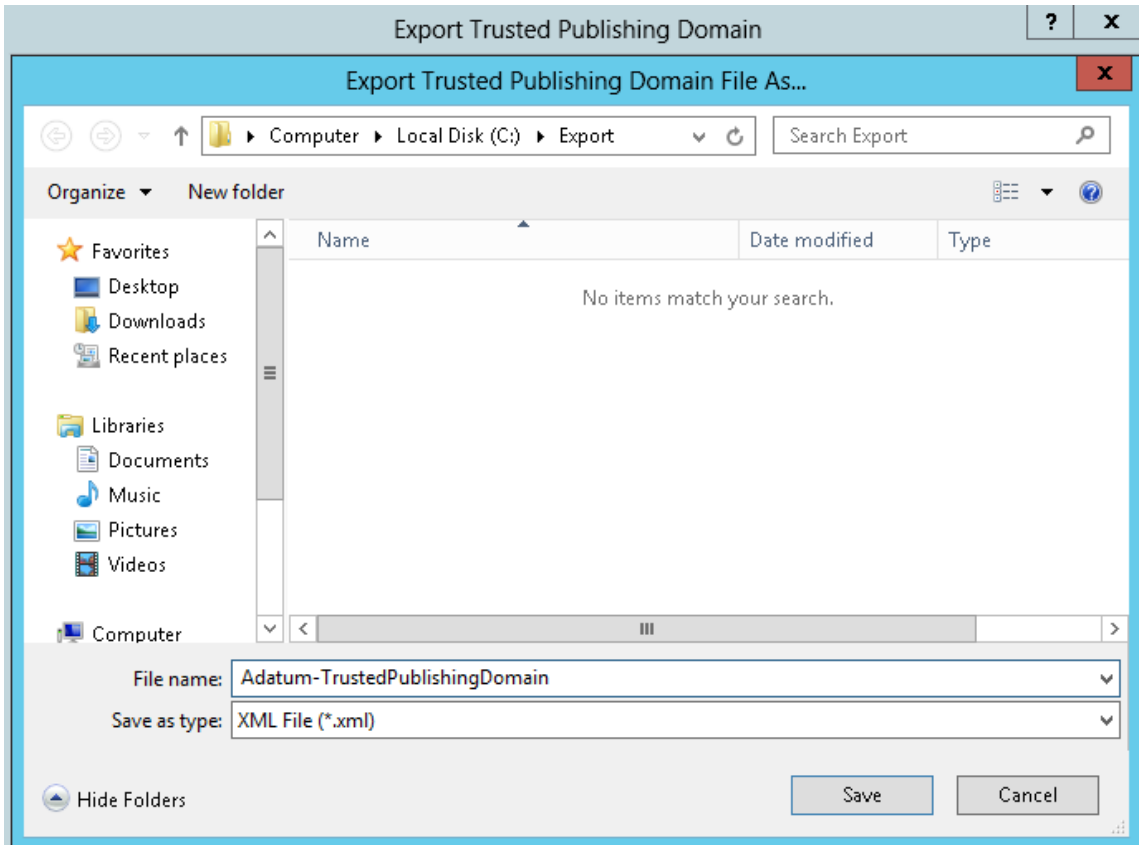
- Exportiere die Domänen-Vertrauensrichtlinie in die Export-Freigabe:

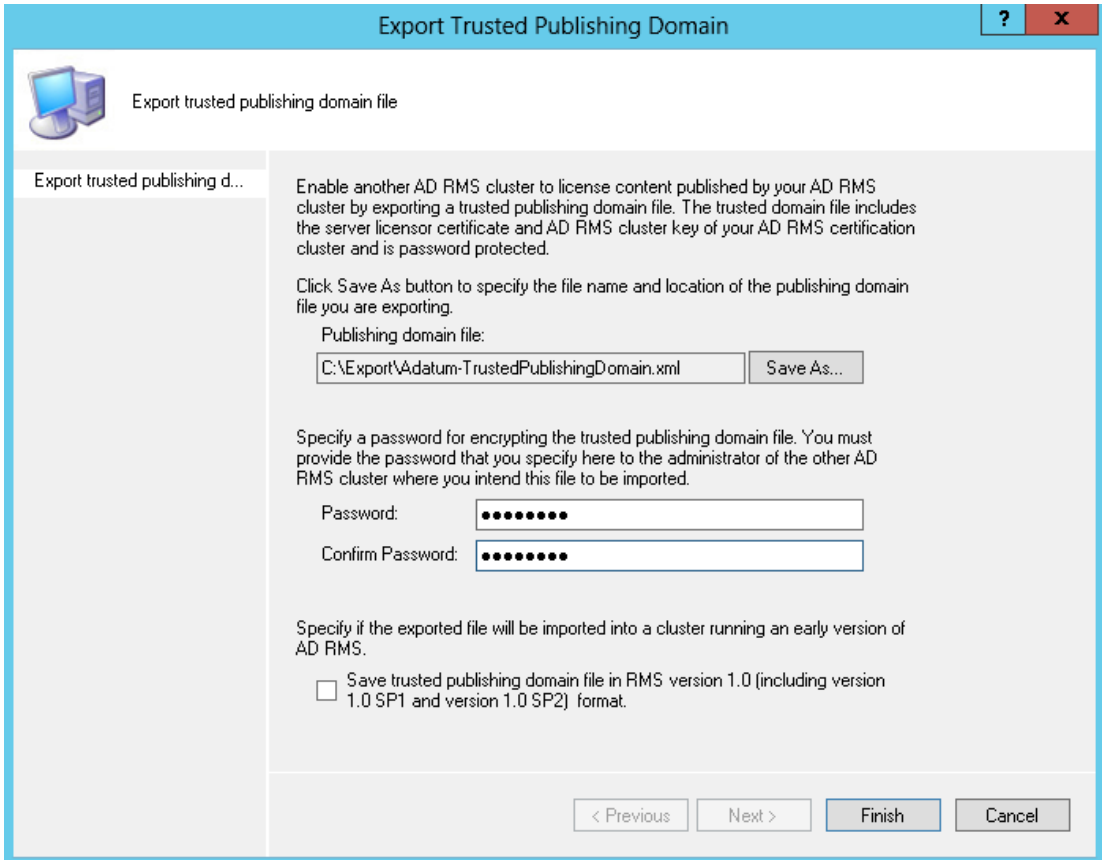




- Exportiere die vertrauenswürdige Veröffentlichungsdomäne :





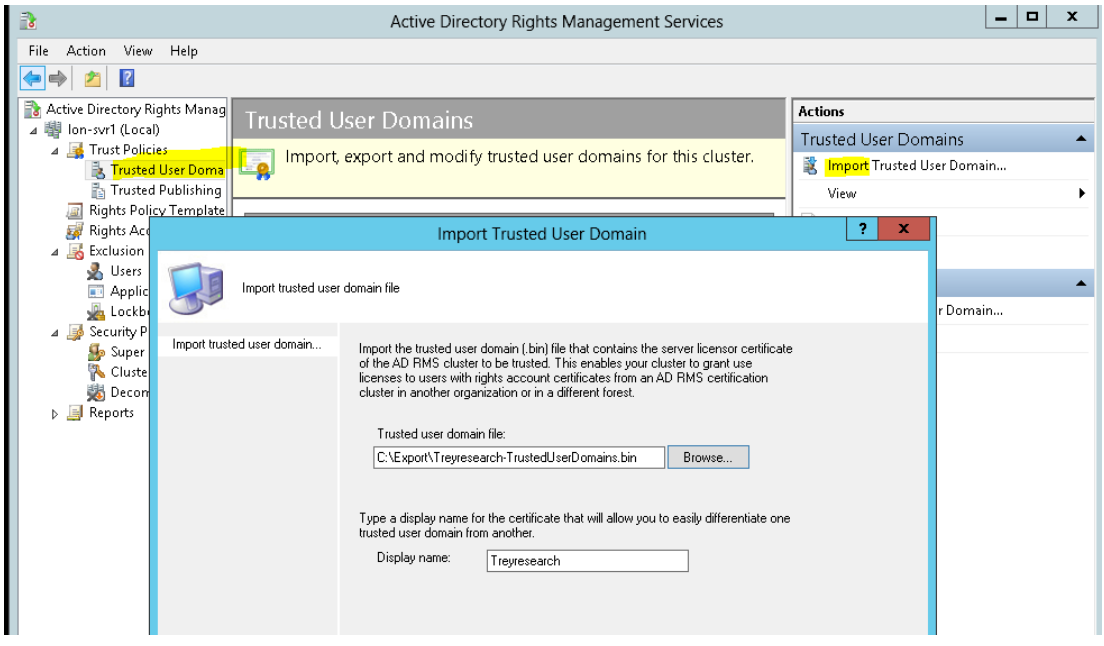


Export der Vertrauensrichtlinie in der Partnerdomäne

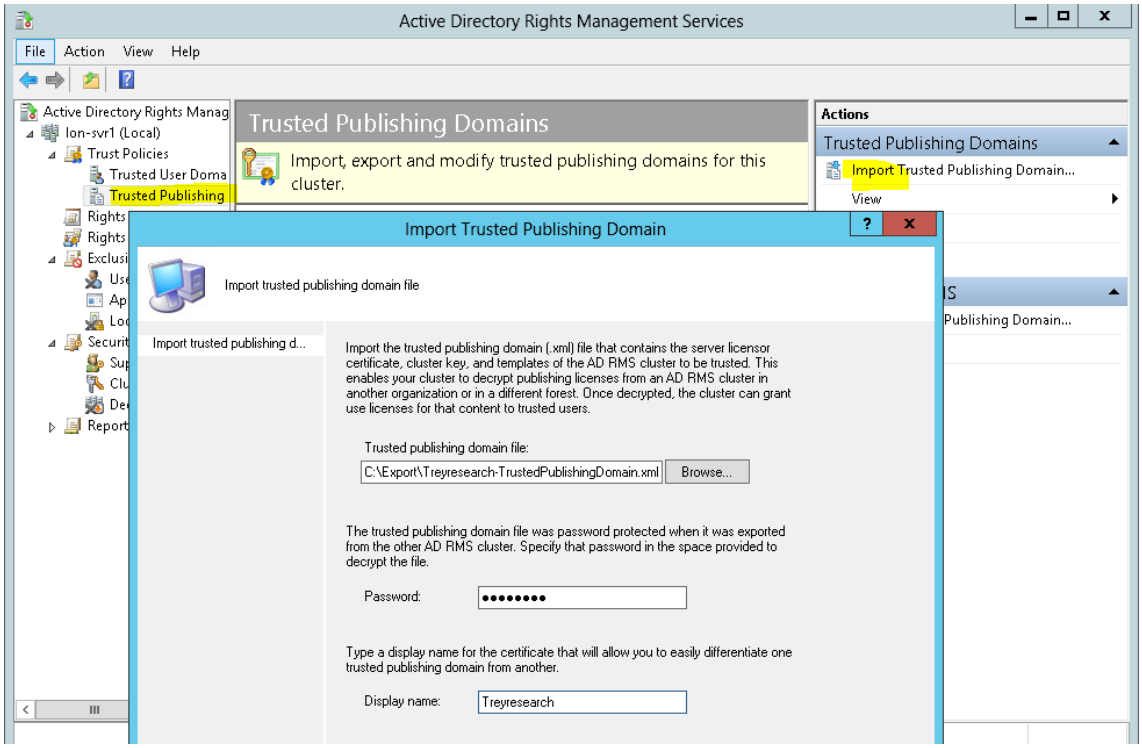
- Die Namensauflösung und die Konnektivität zur Partnerdomäne wird vorausgesetzt
- Exportiere in der Partnerdomäne die Vertrauensrichtlinie in eine Datei Treyresearch-TrustedUserDomains.bin
- Exportiere in der Partnerdomäne die Veröffentlichungsrichtlinie in eine Datei Treyresearch-TrustedPublishingDomain.xml

Import der Vertrauens- und Veröffentlichungsrichtlinien

- Importiere auf LON-SVR1 die Richtliniendateien von Treyresearch:



- Importiere die Veröffentlichungsdomäne:

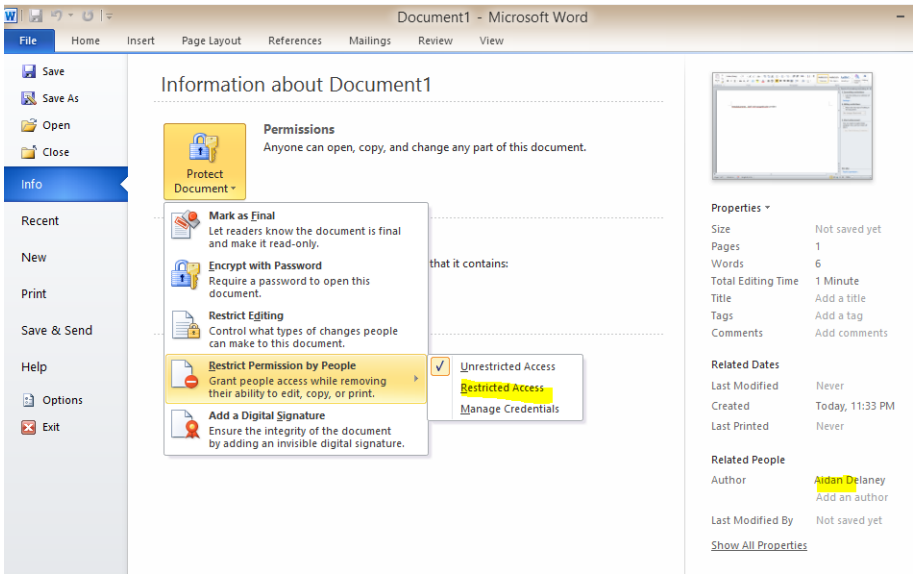


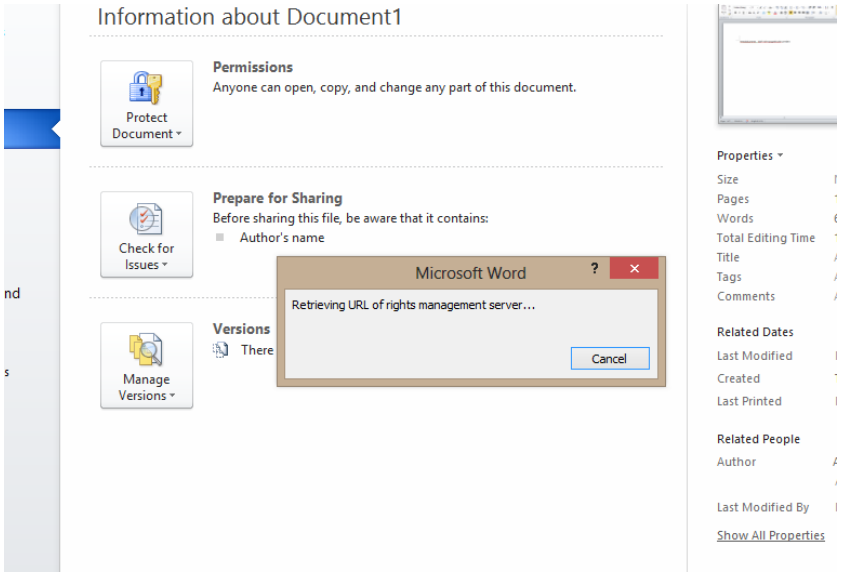
- Analog wird in den RMS von Treyresearch die UserDomain und die ublishingDomain Adatum importiert.

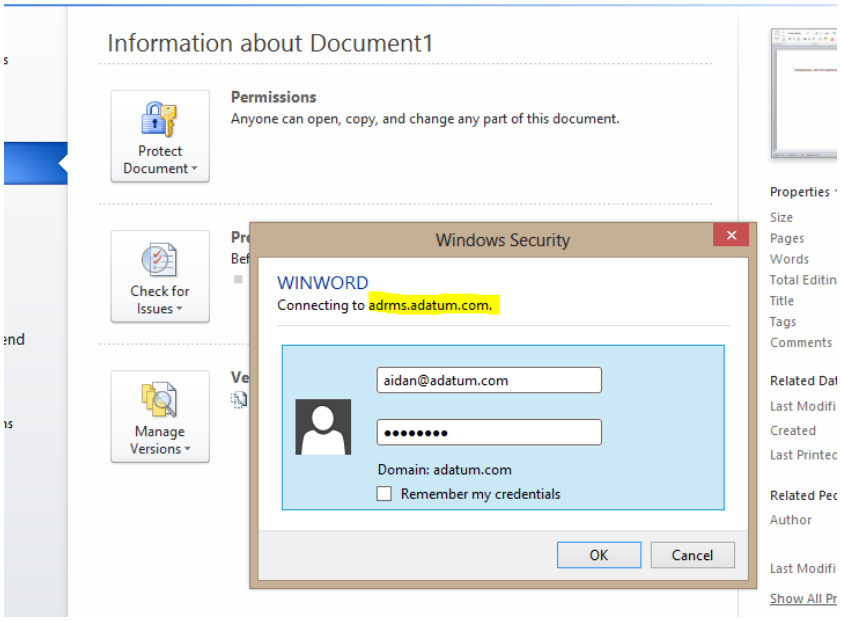
6) Validierung der RMS-Funktionalität – interne Verwendung

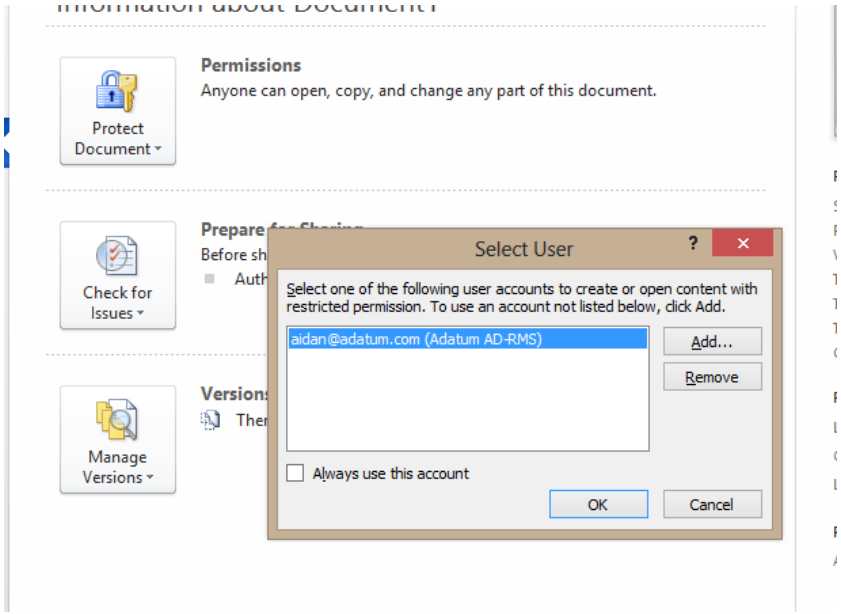
Erstellung eines geschützten Dokumentes für interne Zwecke

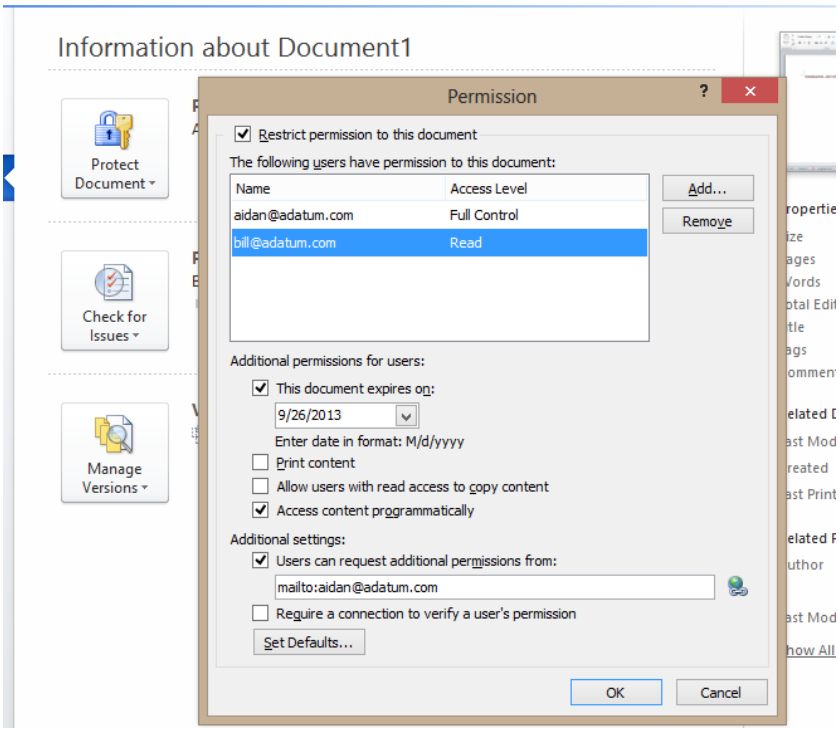
- Anmeldung als Adatum\Aidan auf LON-CL1.adatum.com
- Starte Word 2010
    - Generiere Text
    - Schütze das Dokument:
        - Lesezugriff für Bill@adatum.com:



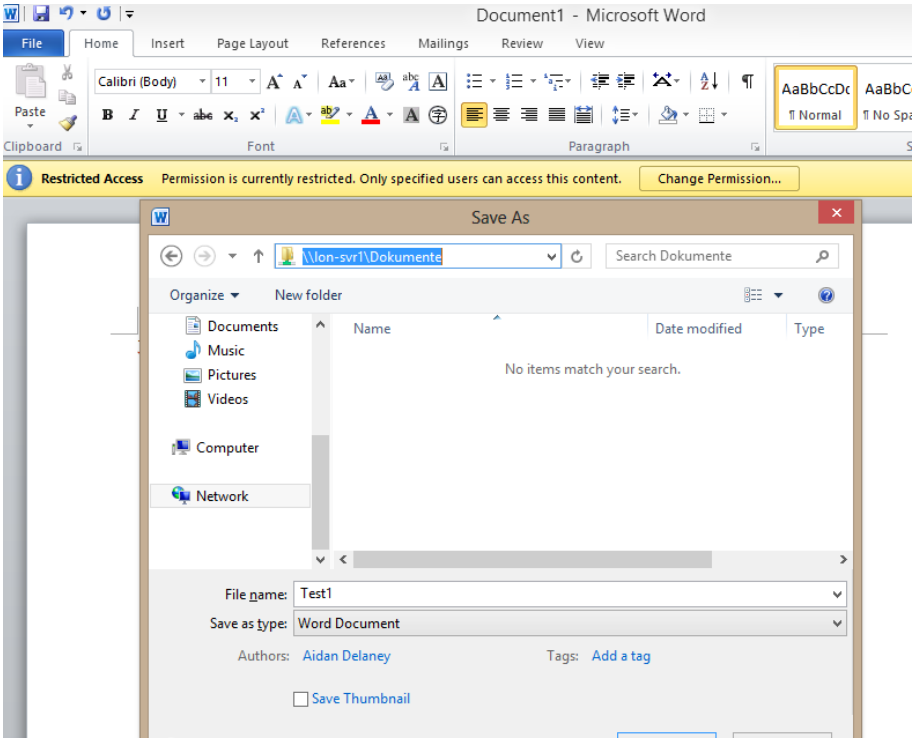

Information about Document1
Protect Document
Permissions
Anyone can open, copy, and change any part of this document.
Check for Issues
Prepare for Sharing
Before sharing this file, be aware that it contains:
Author's name
Manage Versions
Versions
Microsoft Word
Retrieving URL of rights management server...
Cancel
Properties
Size
Pages
Words
Total Editing Time
Title
Tags
Comments
Related Dates
Last Modified
Created
Last Printed
Related People
Author
Last Modified By
Show All Properties


Information about Document1
Protect Document
Permissions
Anyone can open, copy, and change any part of this document.
Check for Issues
Manage Versions
Windows Security
WINWORD
Connecting to adrms.adatum.com.
aidan@adatum.com
Domain: adatum.com
Remember my credentials
OK
Cancel


Protect Document
Permissions
Anyone can open, copy, and change any part of this document.
Check for Issues
Manage Versions
Select User
Select one of the following user accounts to create or open content with restricted permission. To use an account not listed below, click Add.
aidan@adatum.com (Adatum AD-RMS)
Add...
Remove
Always use this account
OK
Cancel

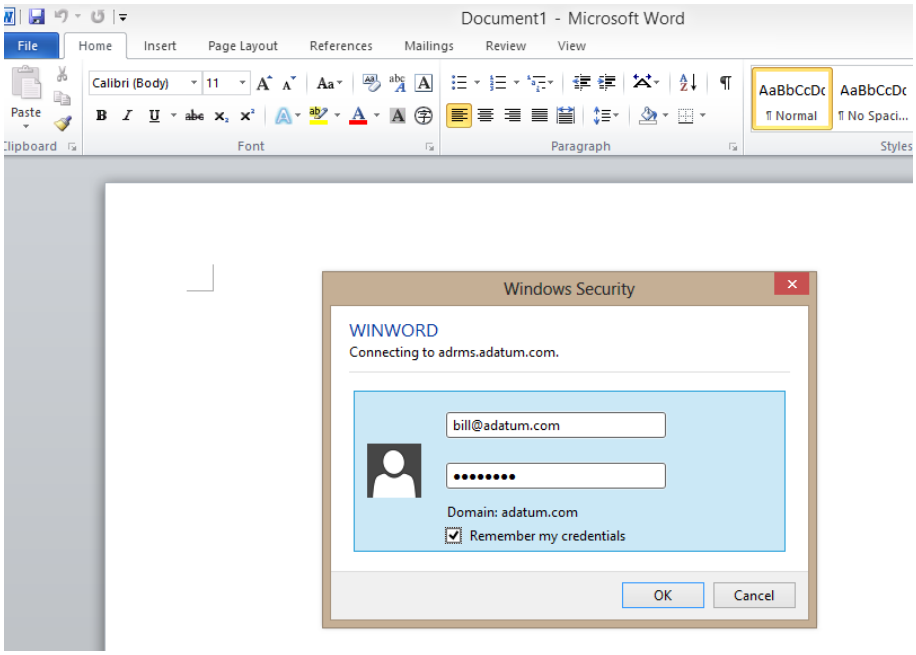


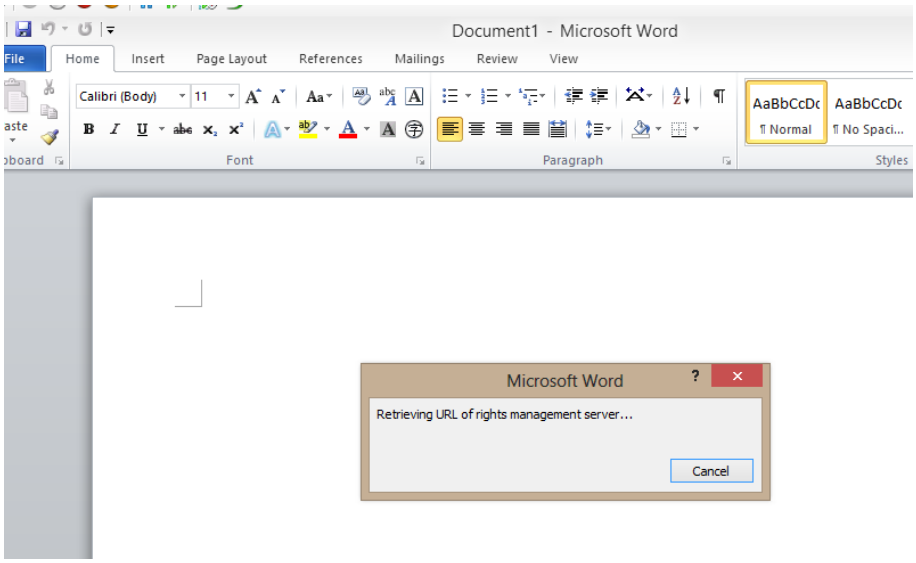
- Speichere die Datei unter \\LON-SVR1\Dokumente\Test1.docx

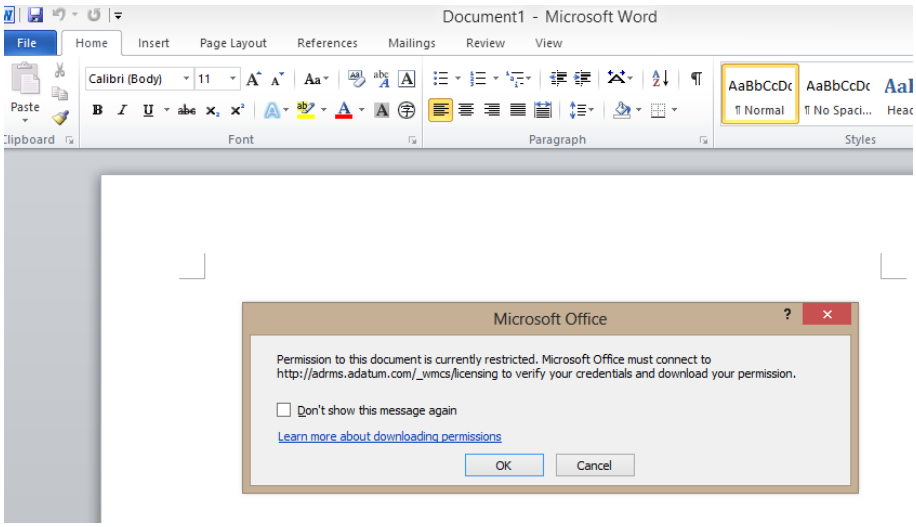


Zugriff auf das interne Dokument (Leserecht)

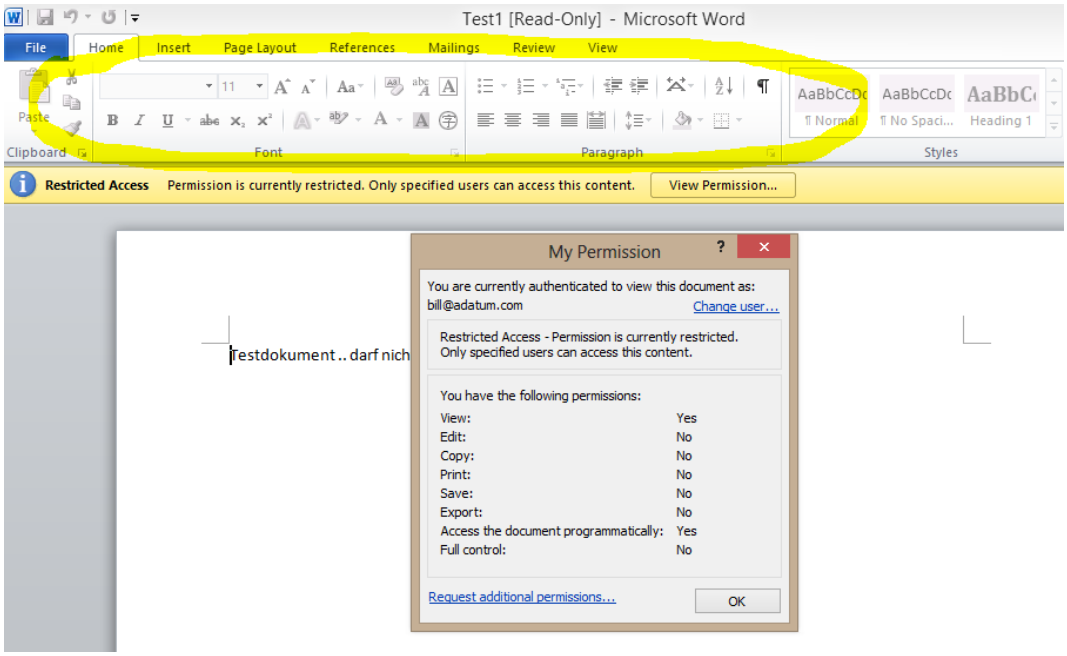
- Anmeldung als Adatum\Bill auf Lon-CL1.adatum.com
- Speichere die Anmeldeinformationen im Office
- Öffne die Datei Test1.docx:


Document1 - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Windows Security
WINWORD
Connecting to adrms.adatum.com.
bill@adatum.com
Domain: adatum.com
Remember my credentials
OK
Cancel


Document1 - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Microsoft Word
Retrieving URL of rights management server...
Cancel

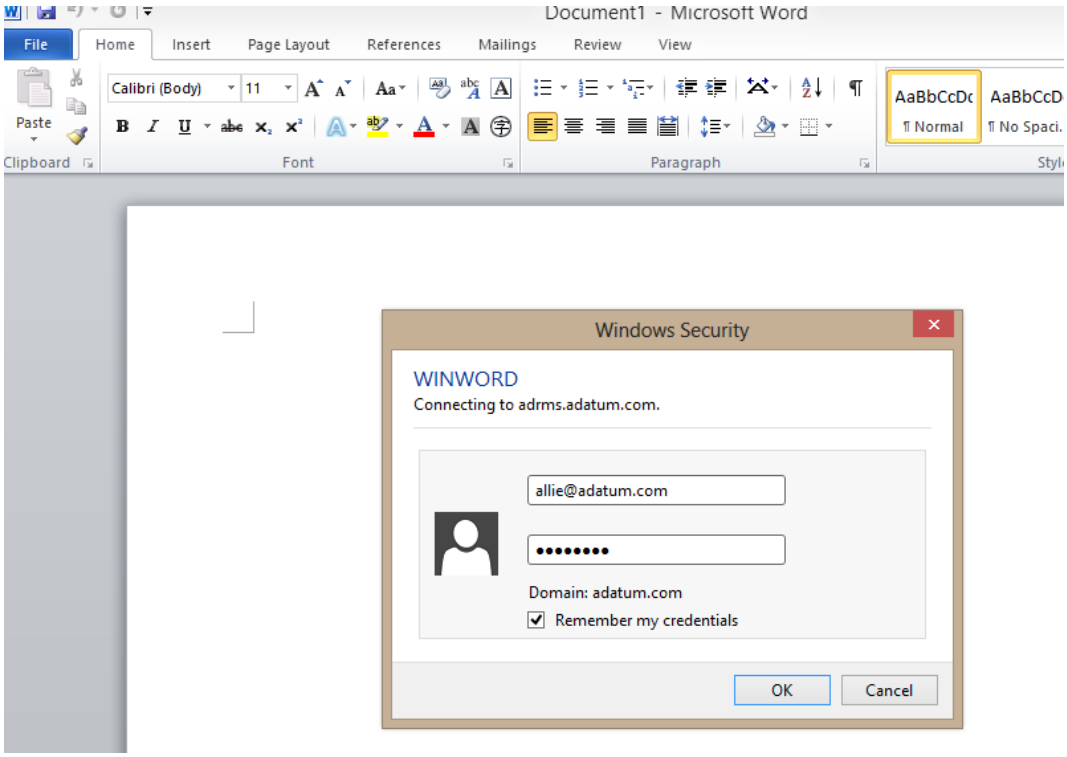

Document1 - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Microsoft Office
Permission to this document is currently restricted. Microsoft Office must connect to http://adrms.adatum.com/_wmcs/licensing to verify your credentials and download your permission.
Don't show this message again
Learn more about downloading permissions
OK
Cancel

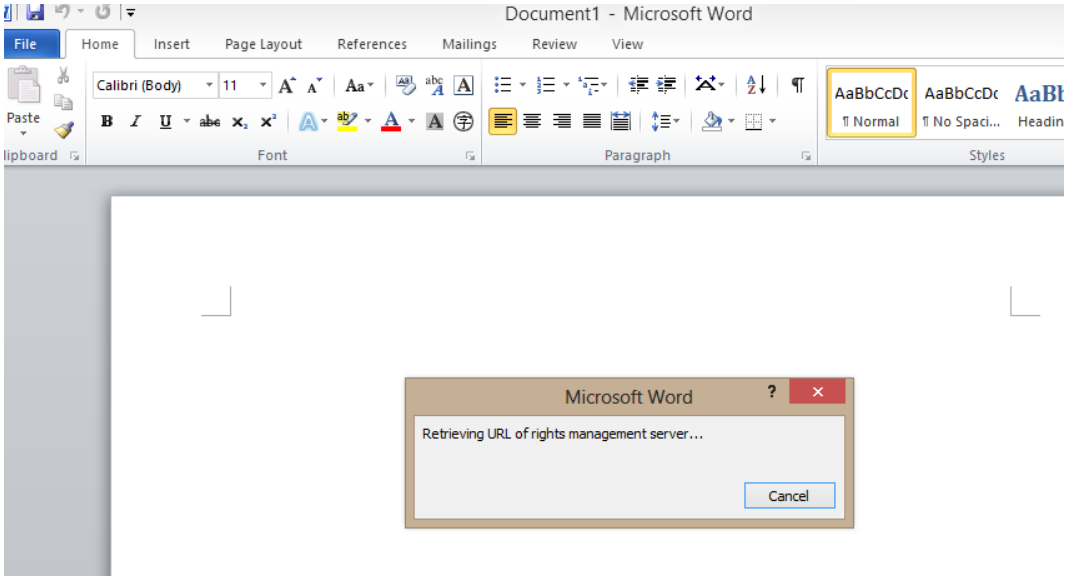
- Versuche Änderungen zu speichern

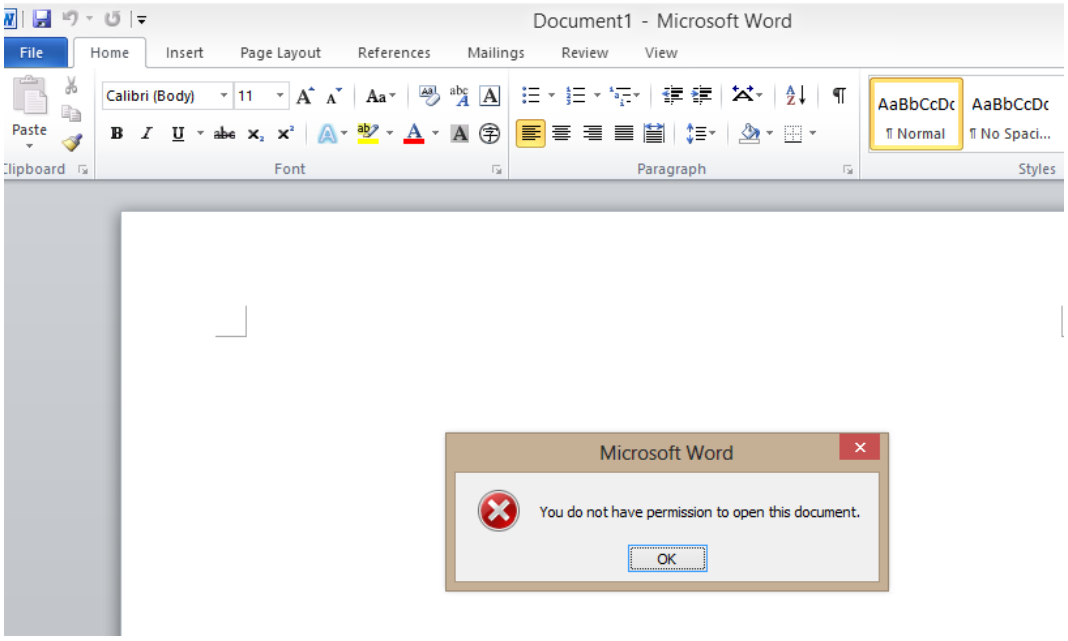


Zugriff auf das interne Dokument (kein Leserecht)

- Anmeldung als Adatum\Allie auf Lon-CL1.adatum.com
- Versuch, das Dokument Test1.docx zu öffnen:





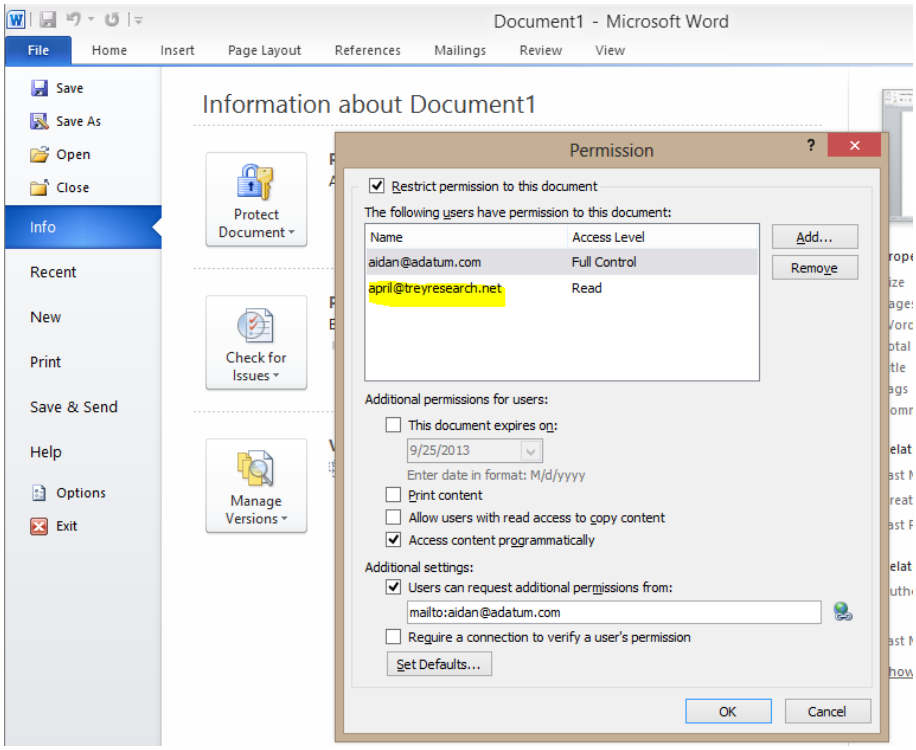


1) Validierung der RMS-Funktionalität – interne Verwendung

Erstellung eines geschützten Dokumentes für externe Personen

- Anmeldung als Adatum\Aidan auf LON-CL1.adatum.com
- Starte Word 2010
    - Generiere Text
    - Schütze das Dokument:

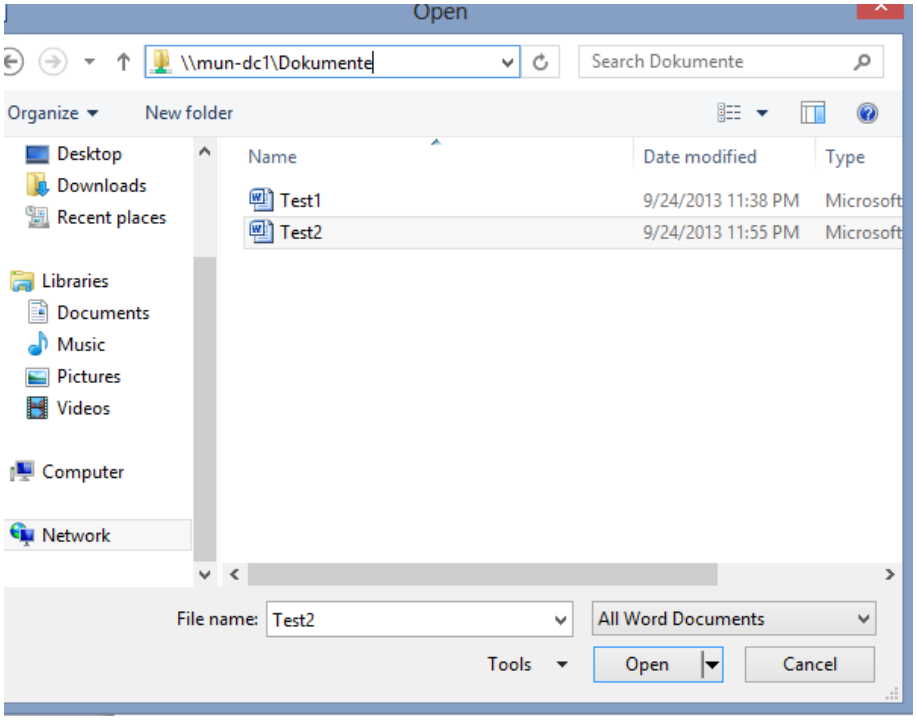
- Lesezugriff für april@treyresearch.net:

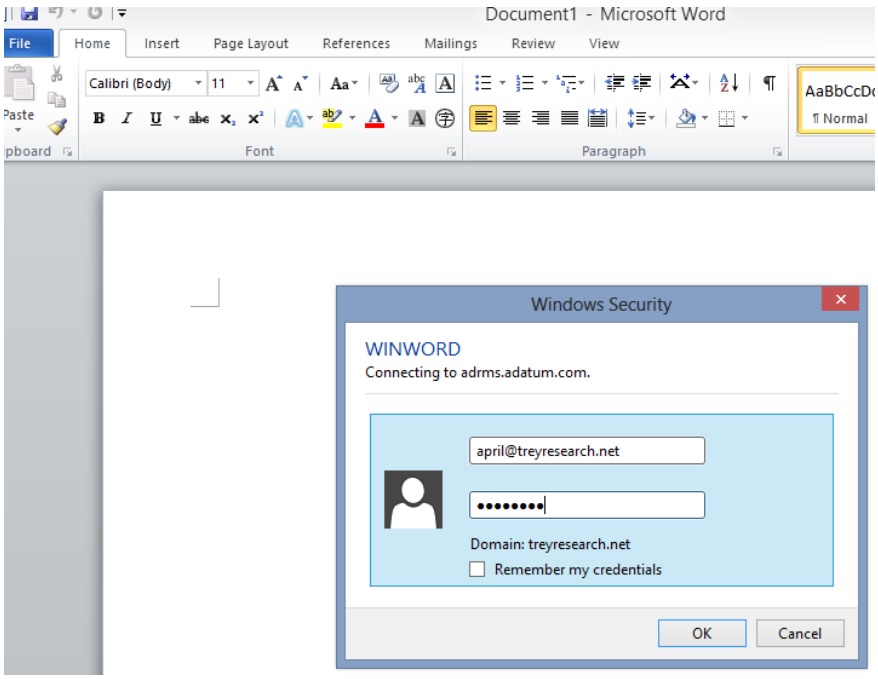


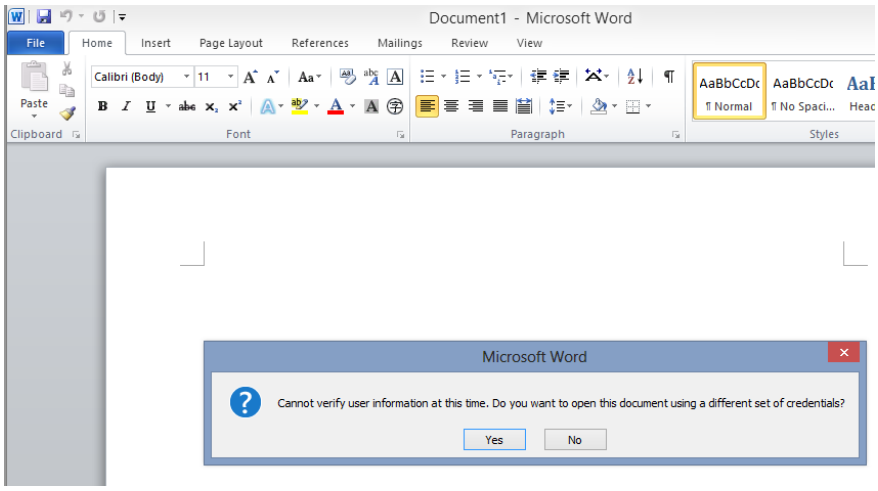
- Speichere das Dokument unter \\LON-SVR1\Dokumente als Test2.docx
- Kopiere das Dokument auf eine Freigabe \\MUN-DC1.treyresearch.net\Dokumente

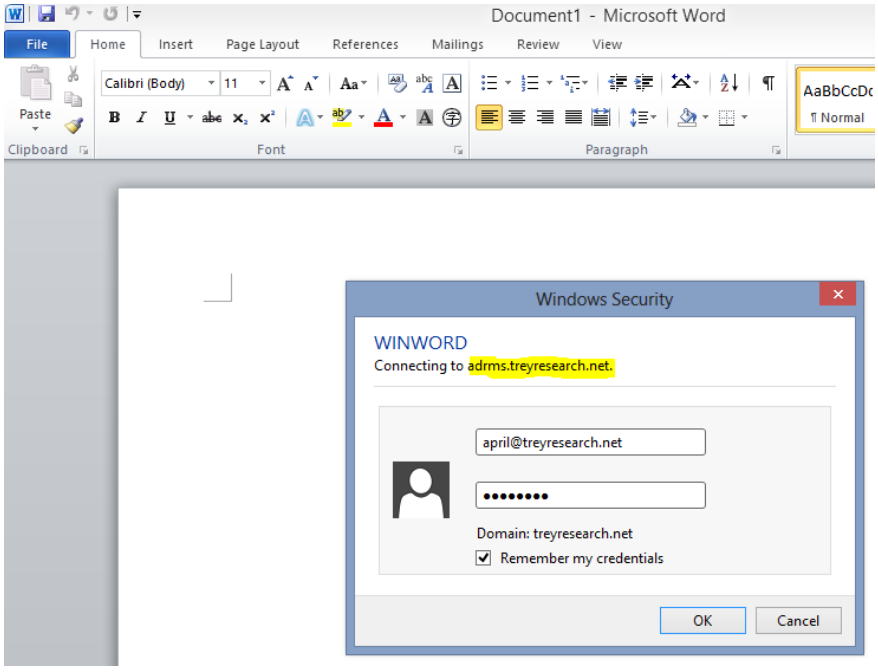
Zugriff auf das externe Dokument (Leserecht)

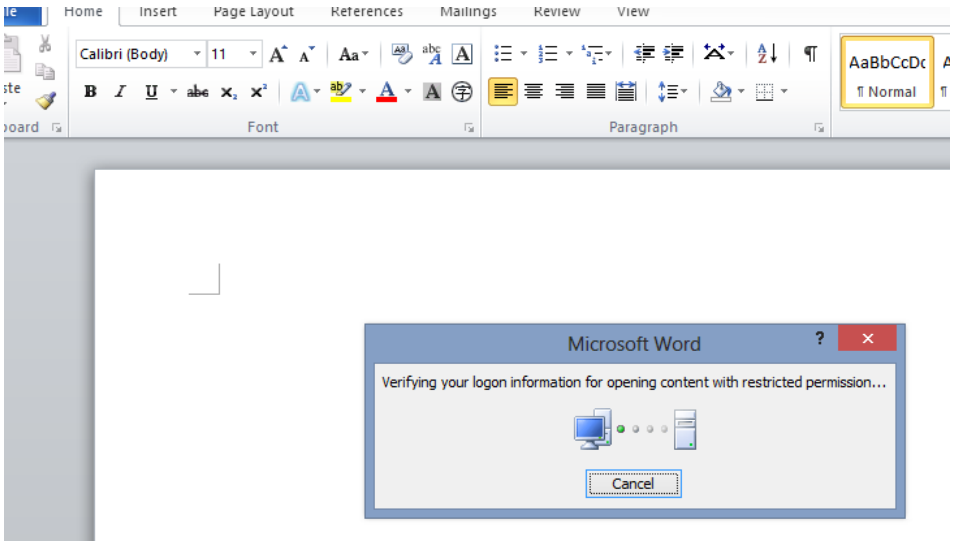
- Anmeldung als TreyResearch\April auf MUN-CL1.adatum.com
- Versuch, das Dokument Test1.docx zu öffnen:

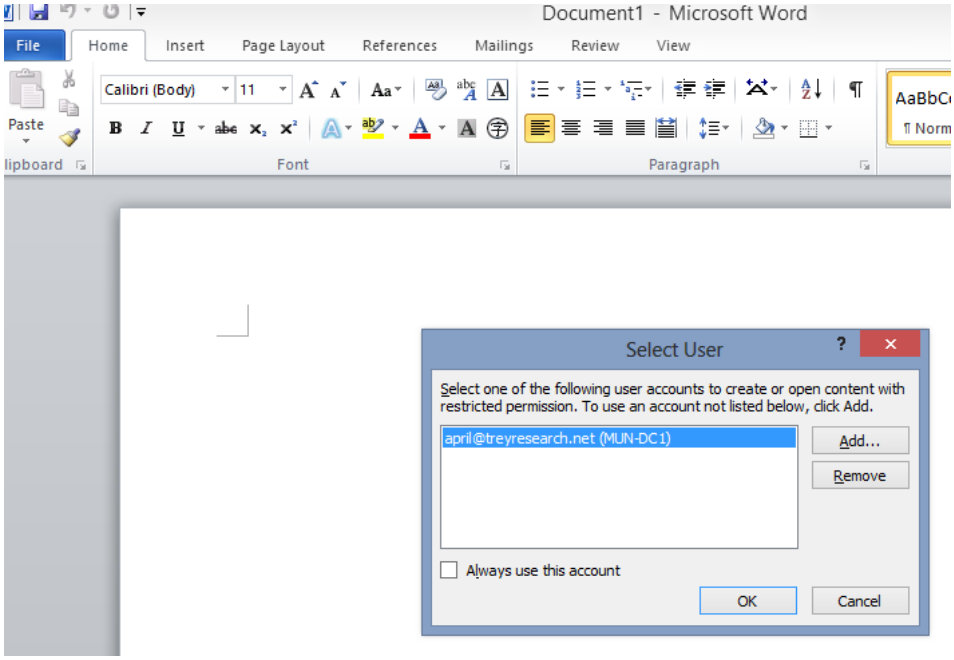


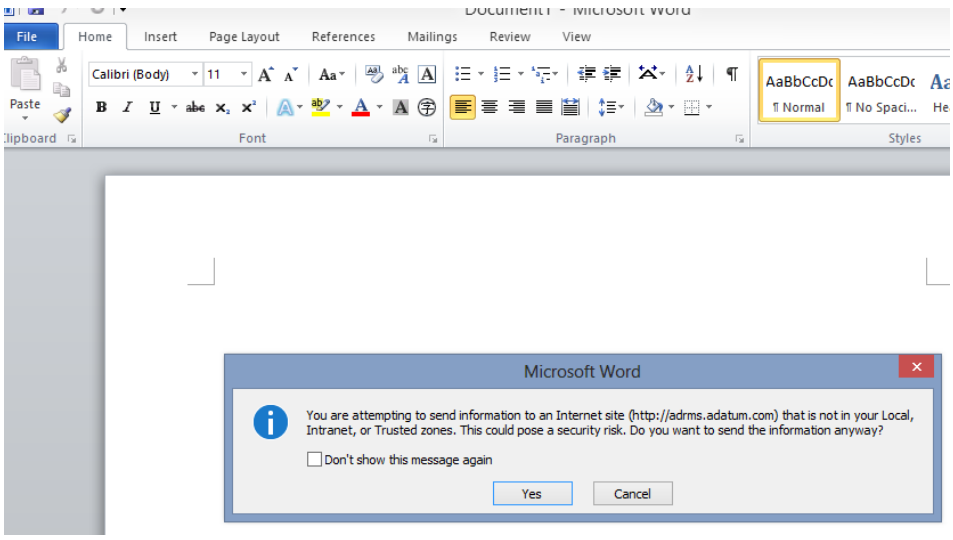

Document1 - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Windows Security
WINWORD
Connecting to adrms.adatum.com.
april@treyresearch.net
Domain: treyresearch.net
Remember my credentials
OK
Cancel

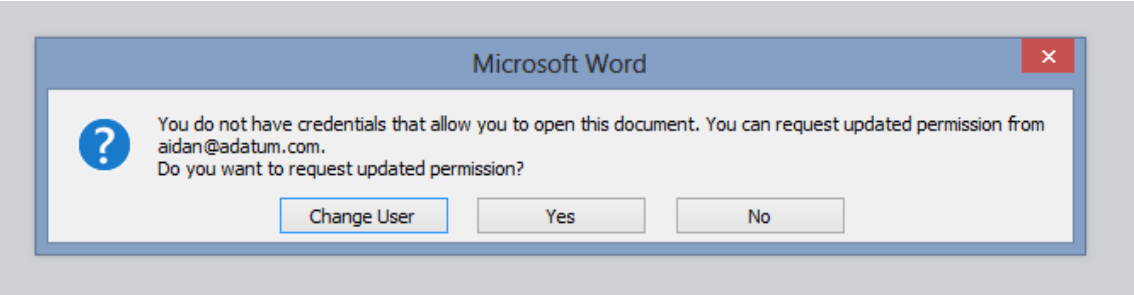

Document1 - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Microsoft Word
Cannot verify user information at this time. Do you want to open this document using a different set of credentials?
Yes
No


Document1 - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Windows Security
WINWORD
Connecting to adrms.treyresearch.net.
april@treyresearch.net
Domain: treyresearch.net
Remember my credentials
OK
Cancel


Home
Insert
Page Layout
References
Mailings
Review
View
Calibri (Body)
11
Font
Paragraph
AaBbCcDc
¶ Normal
Microsoft Word
Verifying your logon information for opening content with restricted permission...
Cancel


Document1 - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Calibri (Body)
11
Font
Paragraph
Select User
Select one of the following user accounts to create or open content with restricted permission. To use an account not listed below, click Add.
april@treyresearch.net (MUN-DC1)
Add...
Remove
Always use this account
OK
Cancel

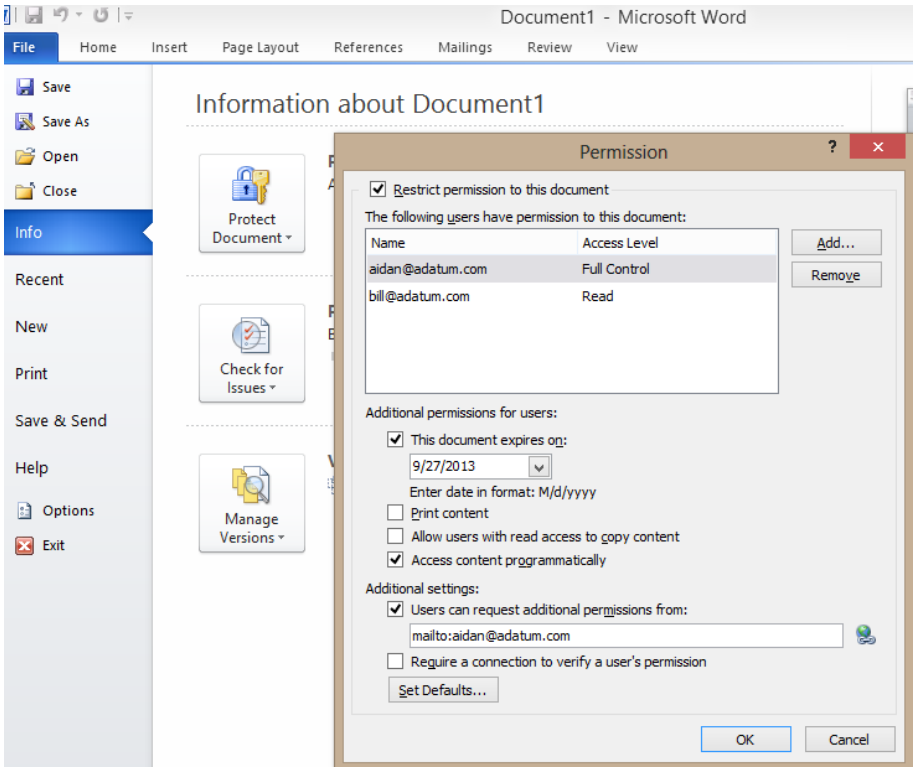

File
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Calibri (Body)
11
Font
Paragraph
Styles
AaBbCcDc
¶ Normal
AaBbCcDc
¶ No Spaci...
Microsoft Word
You are attempting to send information to an Internet site (http://adrms.adatum.com) that is not in your Local, Intranet, or Trusted zones. This could pose a security risk. Do you want to send the information anyway?
Don't show this message again
Yes
Cancel



7) Validierung der Funktionalität bei einem ausgefallenen RMS (intern)

Versuch, eine Datei zu schützen wenn der RMS offline ist

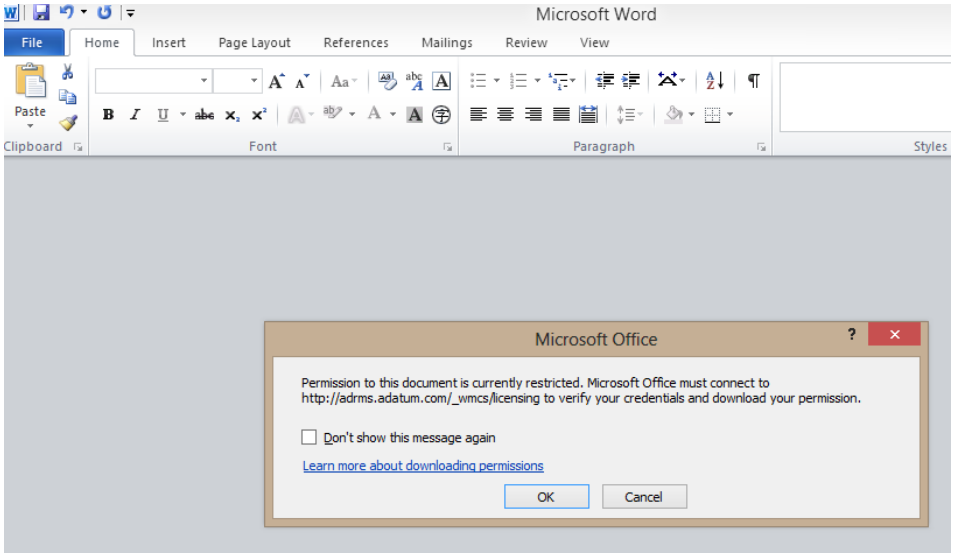
- Anmeldung als Adatum\Aidan auf LON-CL1.adatum.com
- Starte Word 2010
    - Generiere Text
    - Schütze das Dokument:
        - Lesezugriff für bill@adatum.com

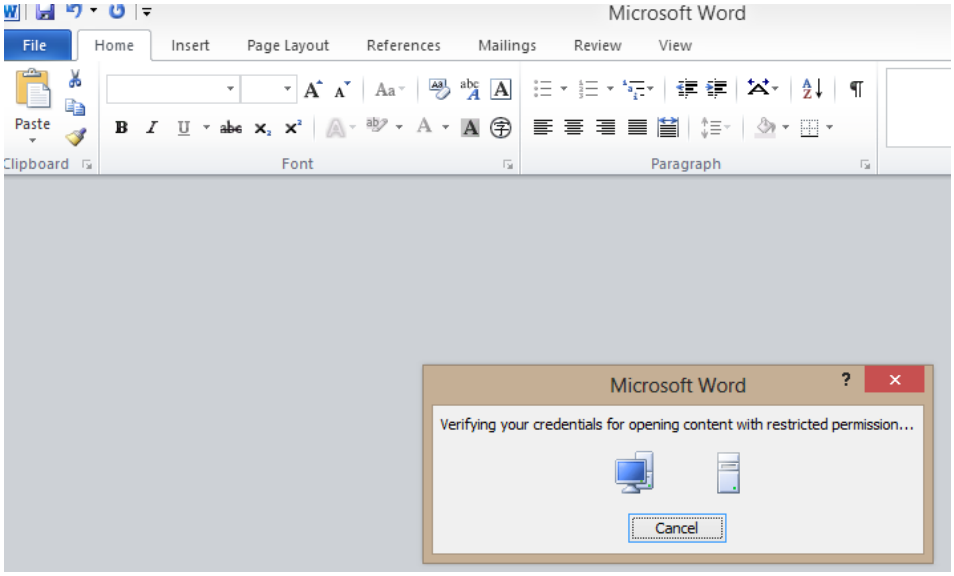


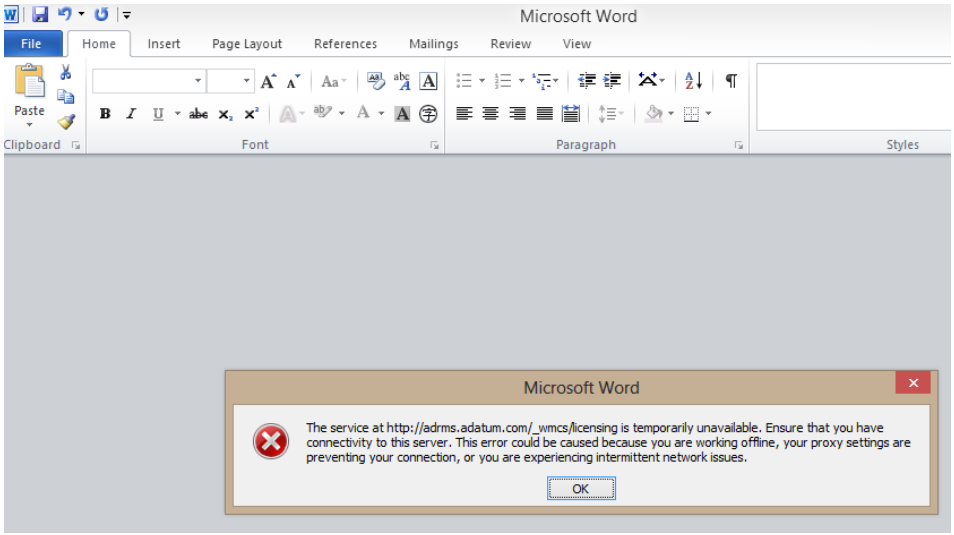
- Speichere das Dokument ... OK

Versuch, eine geschützte Datei zu öffnen, wenn der RMS offline ist

- Anmeldung als Adatum\Bill auf LON-CL1.adatum.com
- Öffne die Datei:



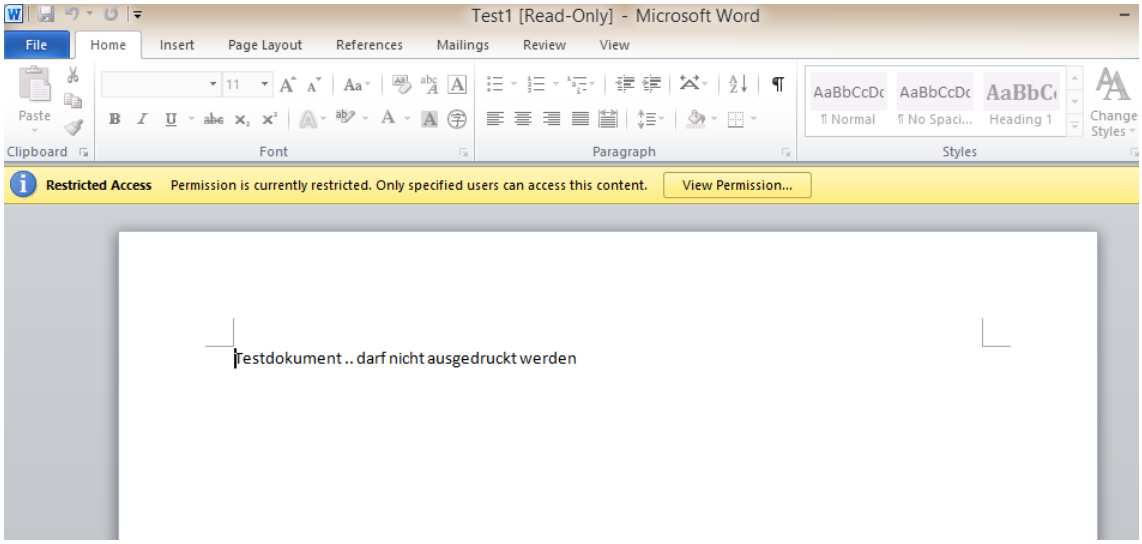




Versuch, eine bekannte geschützte Datei zu öffnen, wenn der RMS offline ist

- Bill hatte das Dokument Test1.docx bereits geöffnet

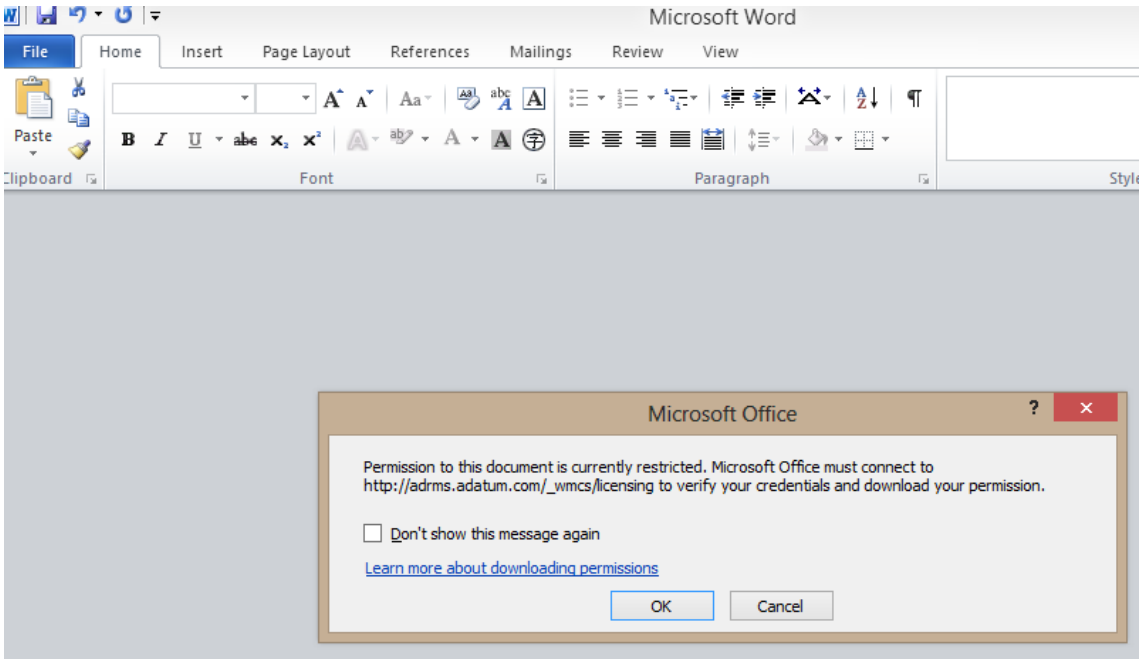
- Erneuter Versuch (die Datei wurde vorher in die eigenen Dokumente kopiert):

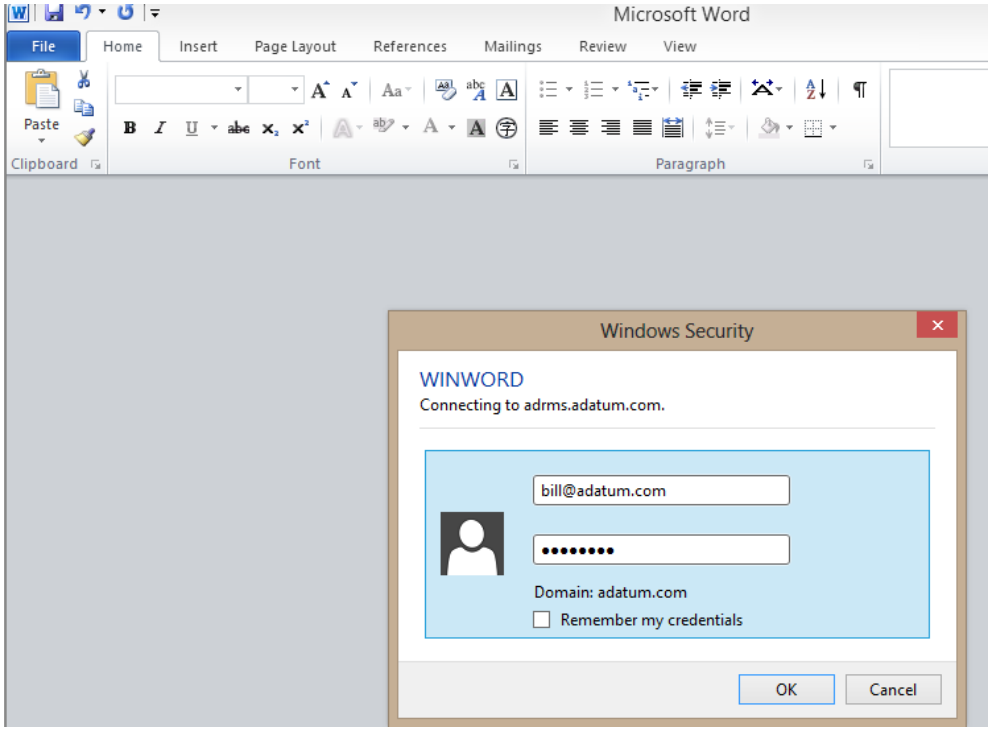


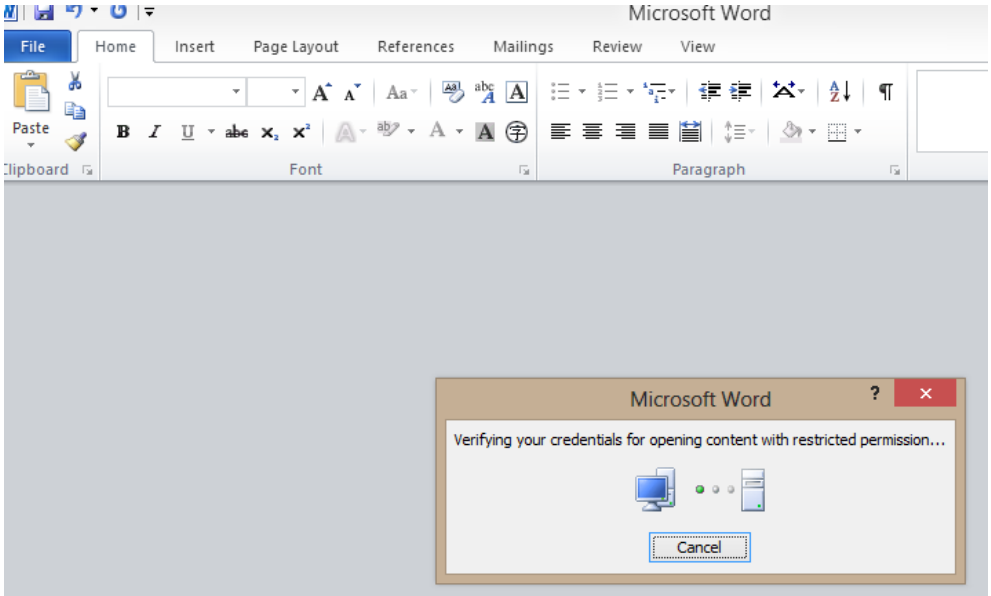
- Da die Richtlinie das zwischenspeichern der Lizenzen am Client für 7 Tage erlaubt, kann Bill das Dokument öffnen

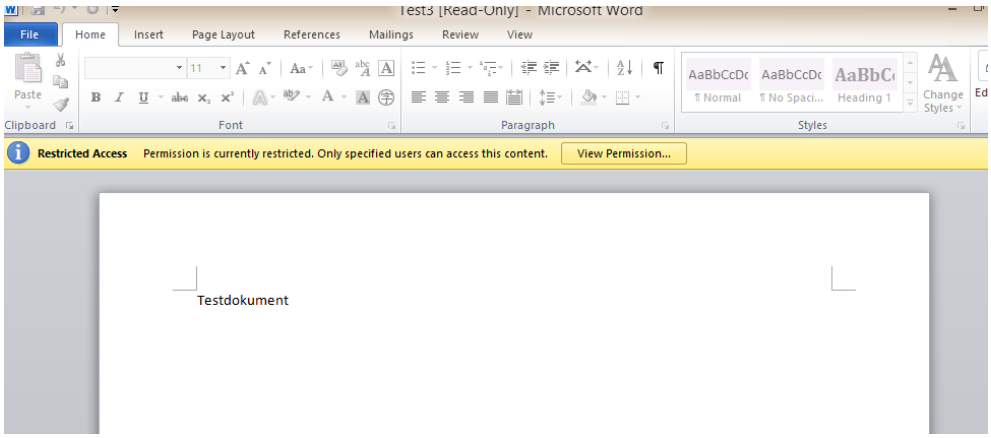
Versuch, die geschützte Datei Test3.docx zu öffnen, nachdem der RMS wieder online ist

- Der RMS ist wieder online
- Bill versucht, die Datei Test3.docx zu öffnen:




Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Clipboard
Font
Paragraph
Windows Security
WINWORD
Connecting to adrms.adatum.com.
bill@adatum.com
Domain: adatum.com
Remember my credentials
OK
Cancel


Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Clipboard
Font
Paragraph
Microsoft Word
Verifying your credentials for opening content with restricted permission...
Cancel


Test3 [Read-Only] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Clipboard
Font
Paragraph
Styles
Restricted Access
Permission is currently restricted. Only specified users can access this content.
View Permission...
Testdokument