Domänenmigration: Vertrauensstellung zwischen Forests im Active Directory einrichten

Domänenmigration: Vertrauensstellung zwischen Forests im Active Directory einrichten

Roland Eich, 12.12.2017
Tags: Active Directory, Migration

In der Praxis kommt es gelegentlich vor, dass AD-Gesamtstrukturen zusammengeführt werden müssen, beispielsweise nach der Fusion von Firmen. Bevor man die Konten für Benutzer und Computer oder Gruppen übernehmen kann, muss man im ersten Schritt eine Vertrauensstellung zwischen den Forests einrichten.

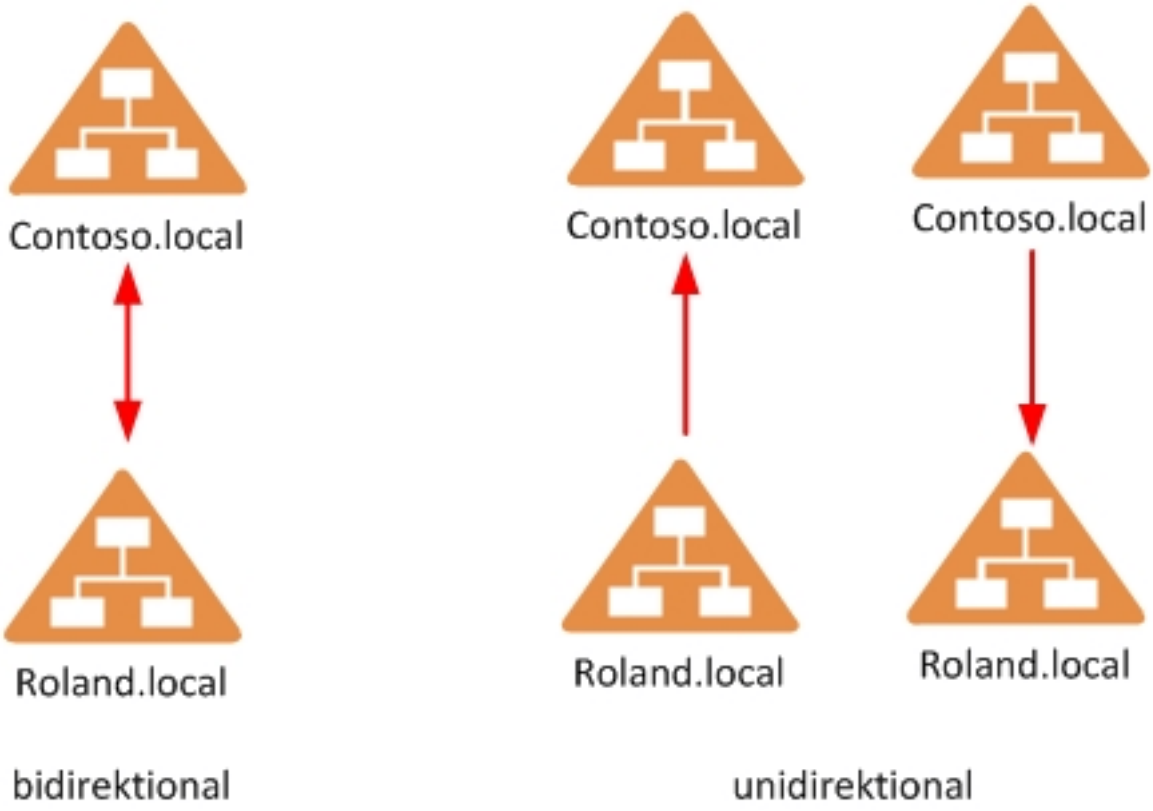
In meinem Beispiel soll eine bestehende Active-Directory-Domäne basierend auf Windows Server 2012 R2 (Contoso.local) auf eine neue Gesamtstruktur migriert werden (Roland.local). Die neue Domäne basiert auf Windows Server 2016.

Achtung! Die folgende Anleitung demonstriert das Vorgehen in einer Testumgebung. Bitte prüfen Sie bei einem produktiv eingesetzten Active Directory genau, warum und zu welchem Zweck Sie eine Vertrauensstellung zwischen zwei Domänen einrichten möchten.

Vertrauensstellungen im Active Directory

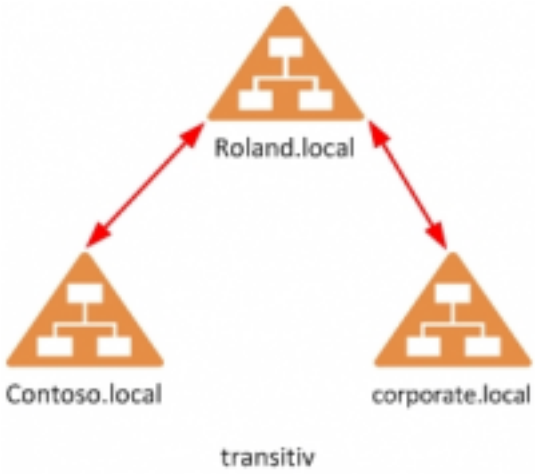
Es gibt im Active Directory zwei Arten von Vertrauensstellungen, die bidirektionale und die unidirektionale:

- Unidirektional ist quasi eine Einbahnstraße. Eine Domäne traut einer anderen, allerdings gilt das nicht umgekehrt. Benutzer, die sich in Contoso.local authentifiziert haben, könnten somit auf Ressourcen in Roland.local zugreifen, aber für User aus Roland.local bleiben die Ressourcen von Contoso.local unzugänglich.
- Bidirektional bedeutet, dass authentifizierte Benutzer beider Domänen in der jeweils anderen Vertrauen genießen. Man könnte auch sagen, die bidirektionale Vertrauensstellung wirkt wie zwei unidirektionale Vertrauens-stellungen.



Unidirektionale versus bidirektionale Vertrauensstellungen im Active Directory

Daneben unterscheidet man noch, ob die Vertrauensstellung transitiv ist oder nicht. Transitiv heißt, dass eine Domäne die Vertrauensstellung auch weiterleiten kann.



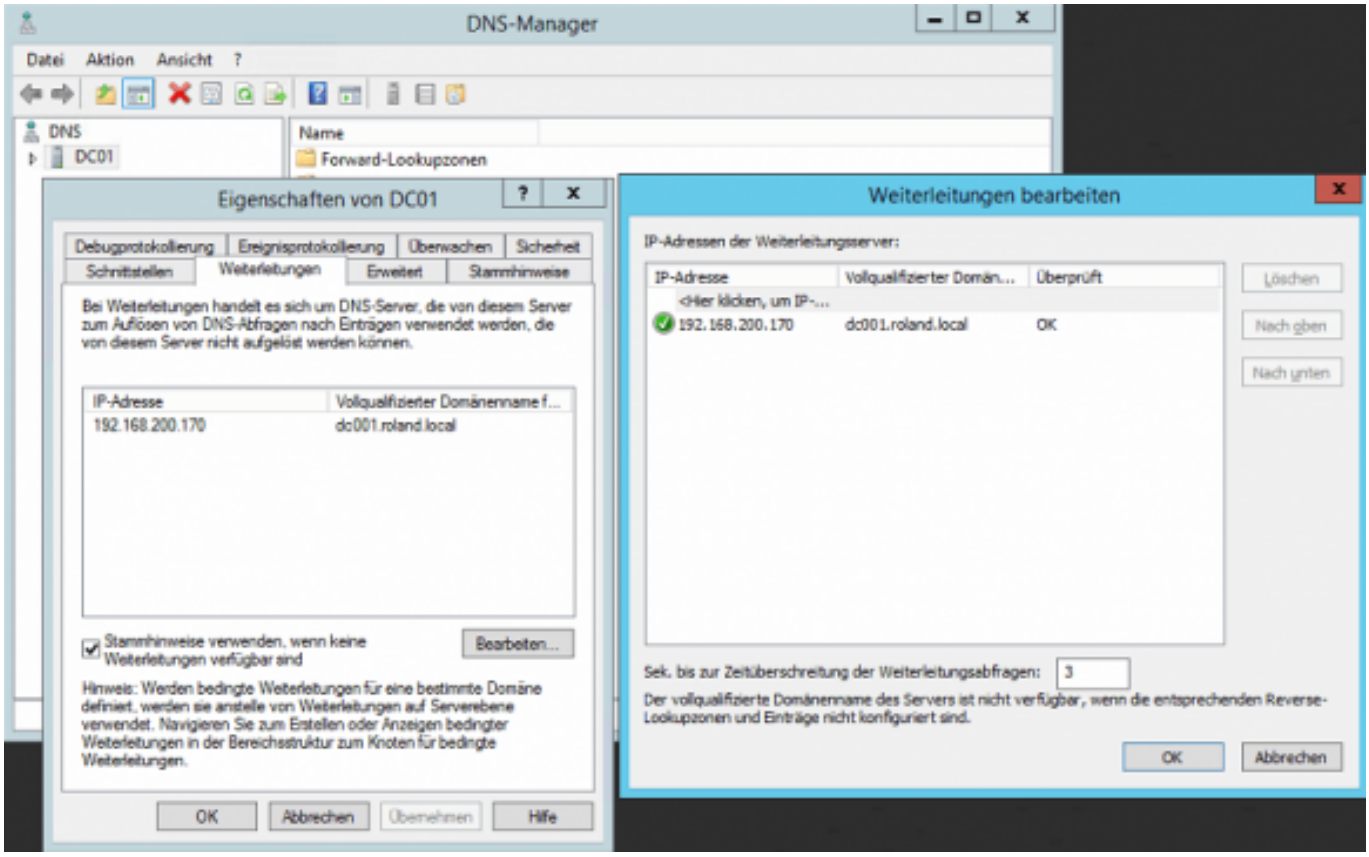
In unserem Beispiel mit den Domänen Contoso.local, Roland.local und Corporate.local würde die Vertrauensstellung von der Domain Contoso.local bis hin zur Domain Corporate.local gehen.

Es muss also nicht zwingend eine Trust-Beziehung von Contoso.local über Roland.local bis zu Corporate.local bestehen, wenn die Domain in der Mitte (Roland.local) eine entsprechende Vertrauensstellung zu beiden Domains hat.

DNS-Weiterleitung einrichten

Bevor es mit der Einrichtung der Vertrauensstellung losgehen kann, muss die Namensauflösung stimmen. Deshalb konfiguriere ich zuerst im DNS-Manager eine wechselseitige Weiterleitung für beide Domänen-Controller/DNS Server, so dass jeder von ihnen die Namen für die Benutzer der jeweils anderen Domäne auflöst.

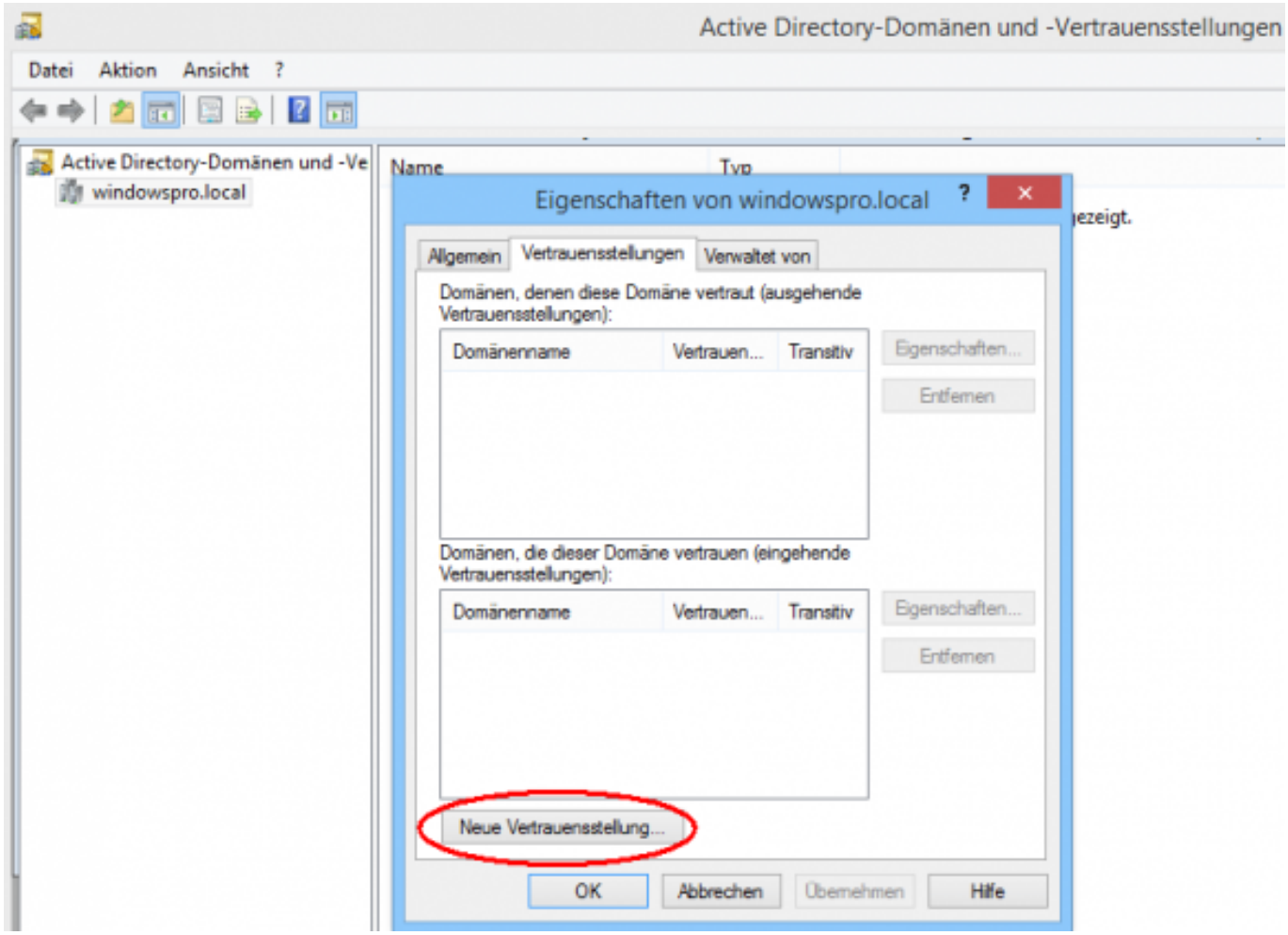
Dafür öffnet man die Eigenschaften der DNS-Server und wechselt zur Registerkarte Weiterleitungen. Die Schaltfläche Bearbeiten startet den Dialog zum Hinzufügen weiterer Name-Server.



DNS-Weiterleitung im MMC-Snapin konfigurieren

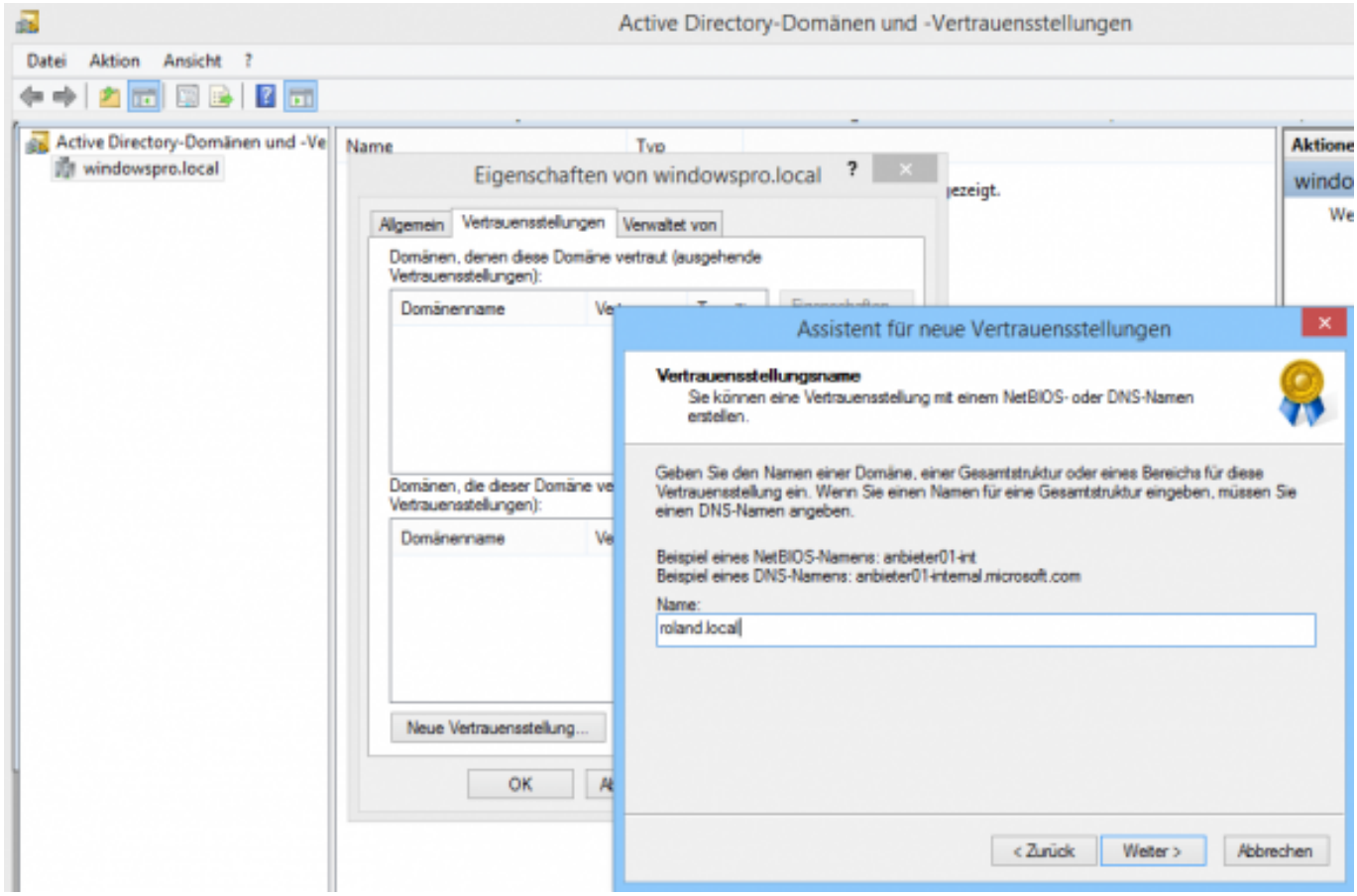
Konfiguration der Vertrauensstellung

Danach kann ich mit dem MMC-Snapin Active Directory Domänen und Vertrauensstellung über den zuständigen Assistenten die Vertrauensstellung einrichten.



Start des Assistenten zur Einrichtung einer neuen Vertrauensstellung

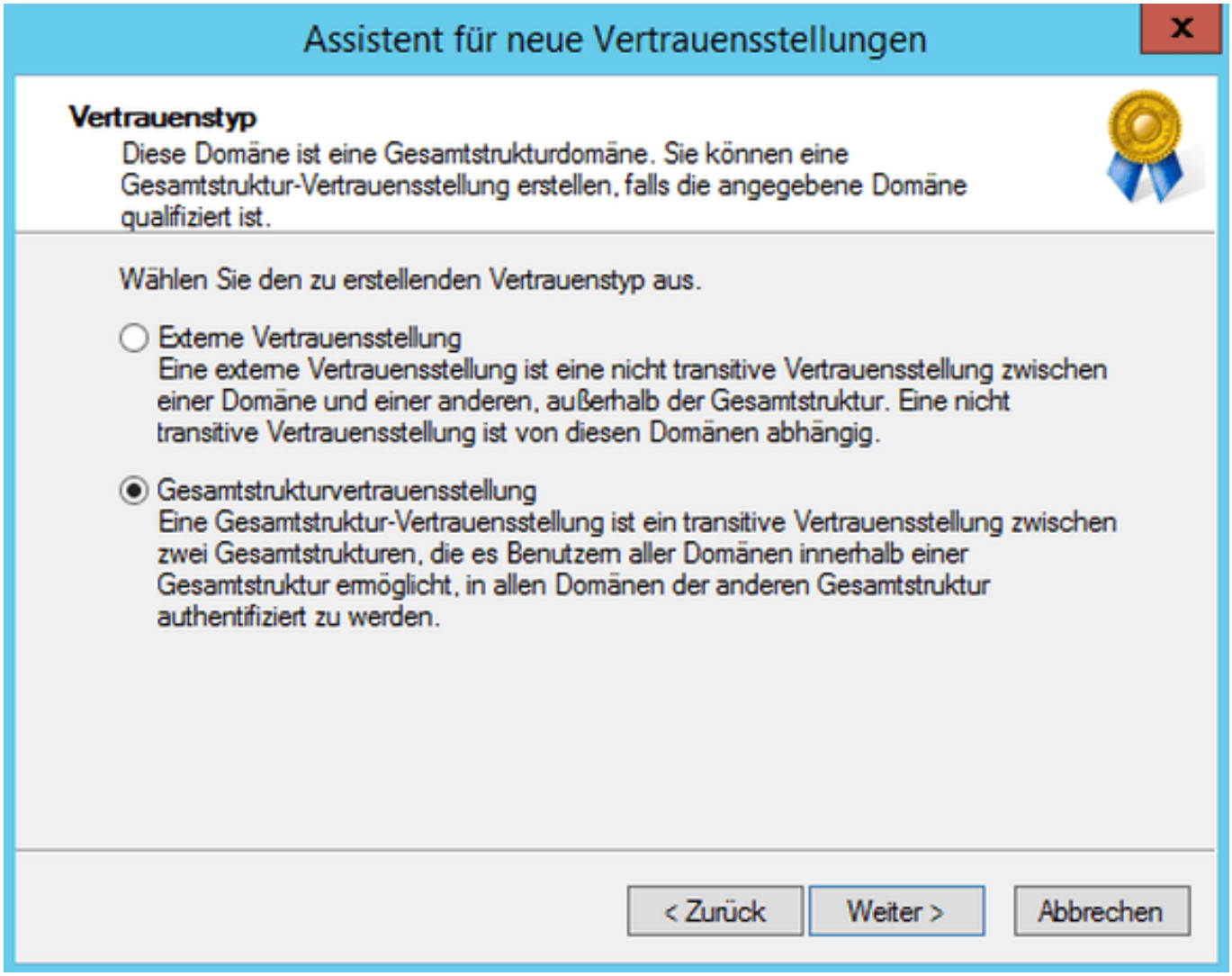
Diesen startet man, indem man die Eigenschaften einer Domäne öffnet und dort die Schaltfläche Neue Vertrauensstellung betätigt.



Name der Domäne für die neue Vertrauensbeziehung eingeben

Hier gebe ich nun den Name der neuen Domäne (Zieldomäne) ein.

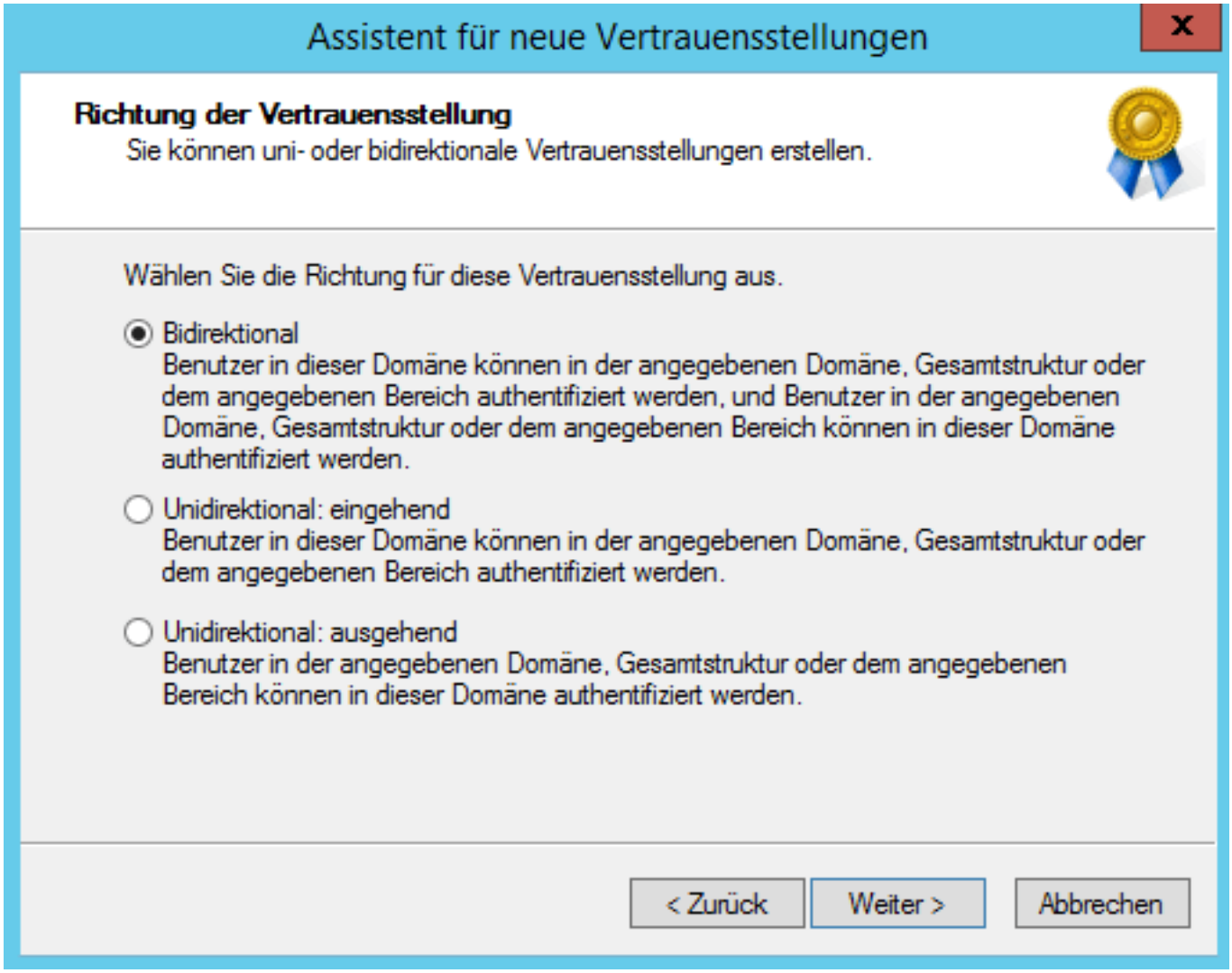
Im nächsten Fenster muss nun Externe
Vertrauensstellung und Gesamtstrukturvertrauensstellung zu Auswahl stehen. Sollte dies nicht der Fall sein, konnte die Zieldomäne nicht richtig aufgelöst werden.



Auswahl der Vertrauenstyps für die neue Vertrauensstellung

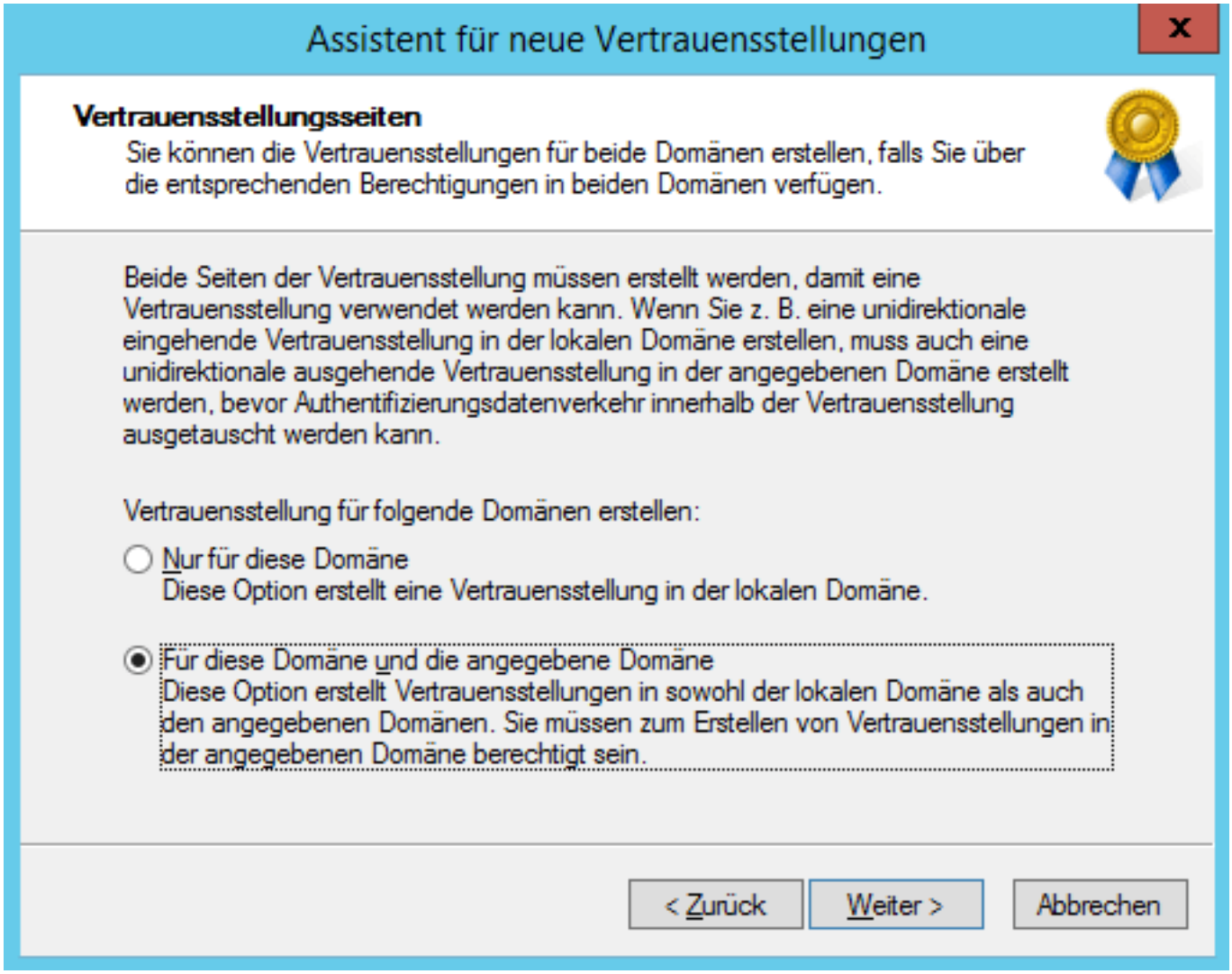
Wenn Sie, wie im oberen Bild ersichtlich, eine transitive Vertrauensstellungen nicht möchten, so dass ggf. auch noch andere Domänen Zutritt zu Ihrem Netzwerk erhalten, so haben Sie jetzt die Möglichkeit, Externe Vertrauensstellung auszuwählen.

Im folgenden Fenster entscheide ich mich nun, ob es eine bidirektionale oder eine unidirektionale Vertrauensstellung sein soll. In meinem Fall möchte ich, dass die beiden Domänen sich voll vertrauen und wähle bidirektional.



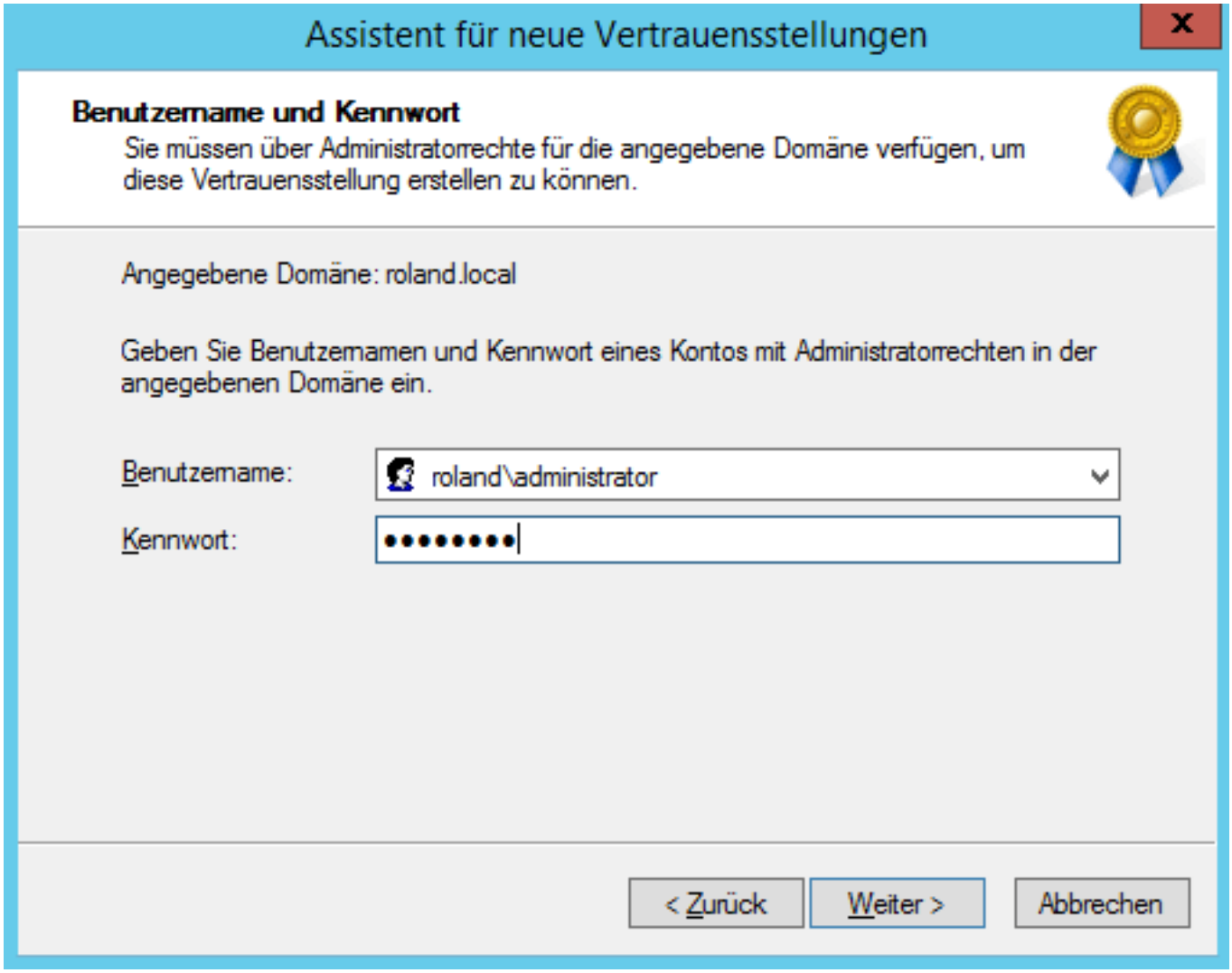
Auswahl zwischen einer neuen uni- oder bidirektionalen Vertrauensstellung

Im nächsten Schritt könnten wir uns auf Nur für diese Domäne beschränken. Das würde aber dann bedeuten, dass wir diesen ganzen Vorgang auf der anderen Domäne nochmal machen müssen. Daher wählen wir hier Für diese Domäne und die angegebene Domäne.



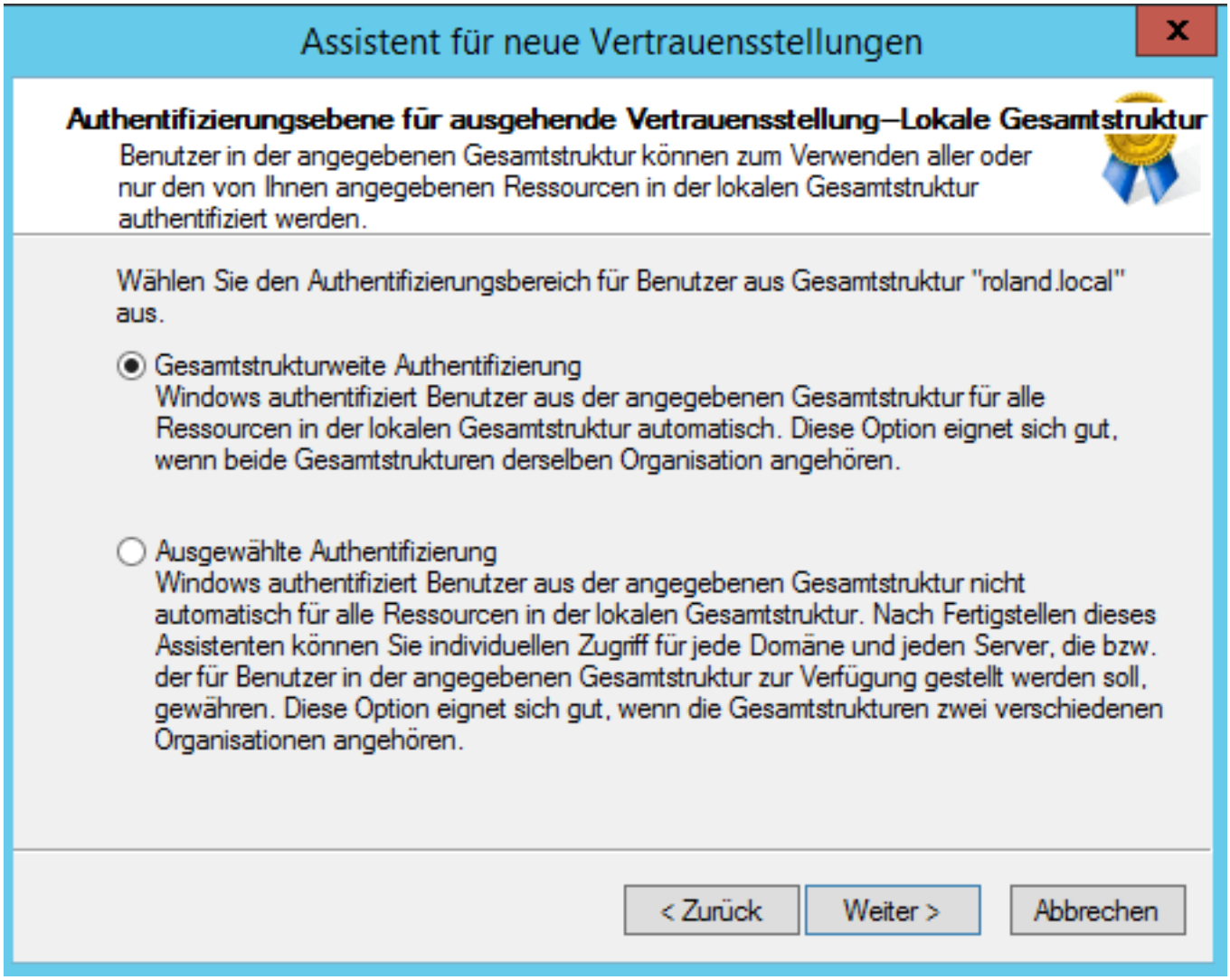
Festlegung, ob die Vertrauensstellung nur für diese oder beiden Domänen gelten soll.

Damit die Vertrauensstellung auch in der anderen Domäne (in unserem Fall roland.local) angelegt werden kann, benötigen wir einen Benutzer mit Administratorrechten.



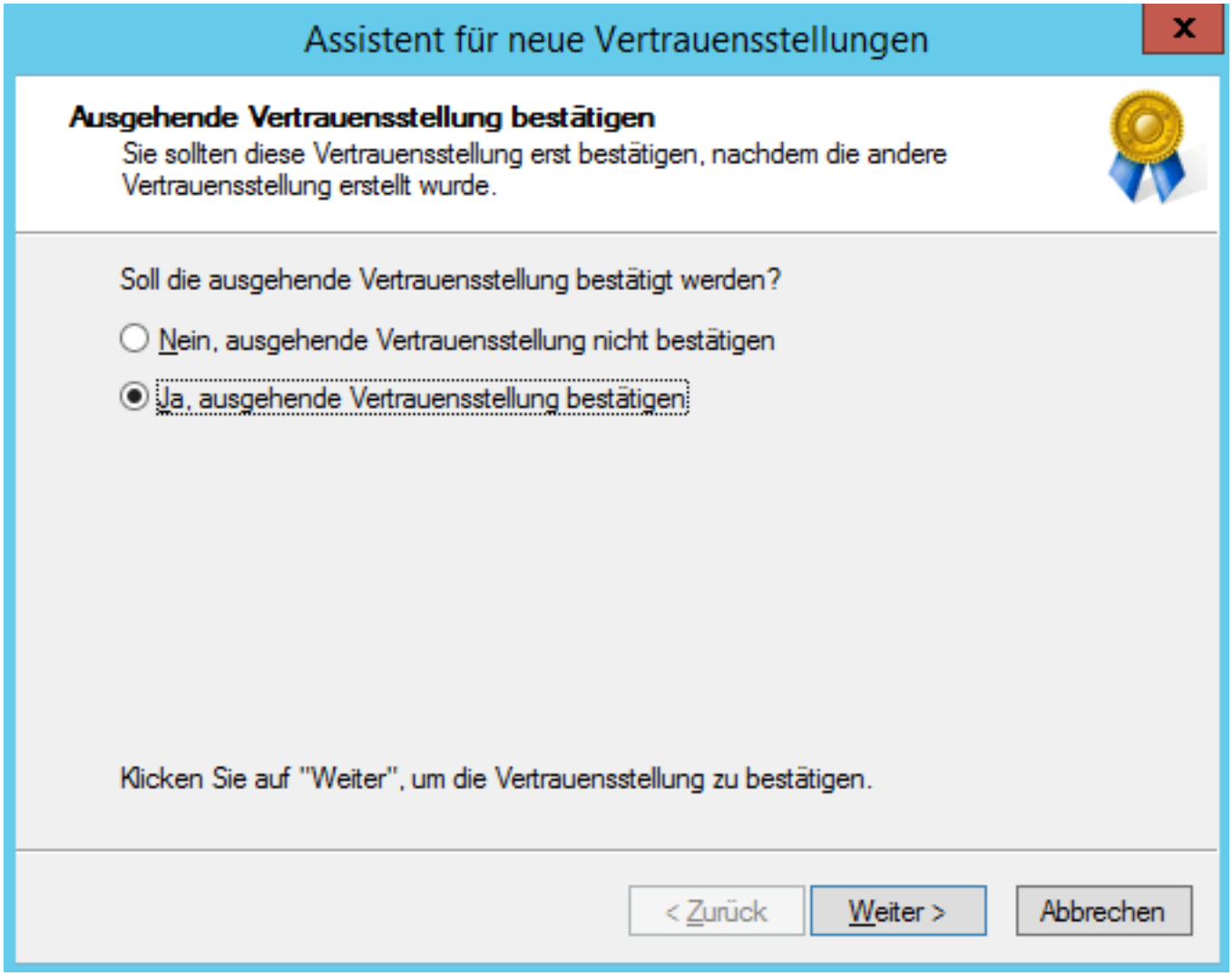
Authentifizierung eines Administrators für das Einrichten einer neuen Vertrauensstellung

In nächsten Dialog könnten wir den Zugriff zwischen den Domänen nur für bestimme Ressourcen zulassen. Ich möchte hier aber vollen Zugriff geben (Achtung: Es wird zweimal gefragt, jeweils einmal für jede Gesamtstruktur).



Wahl der Authentifizierungsebene für die neue Vertrauensstellung

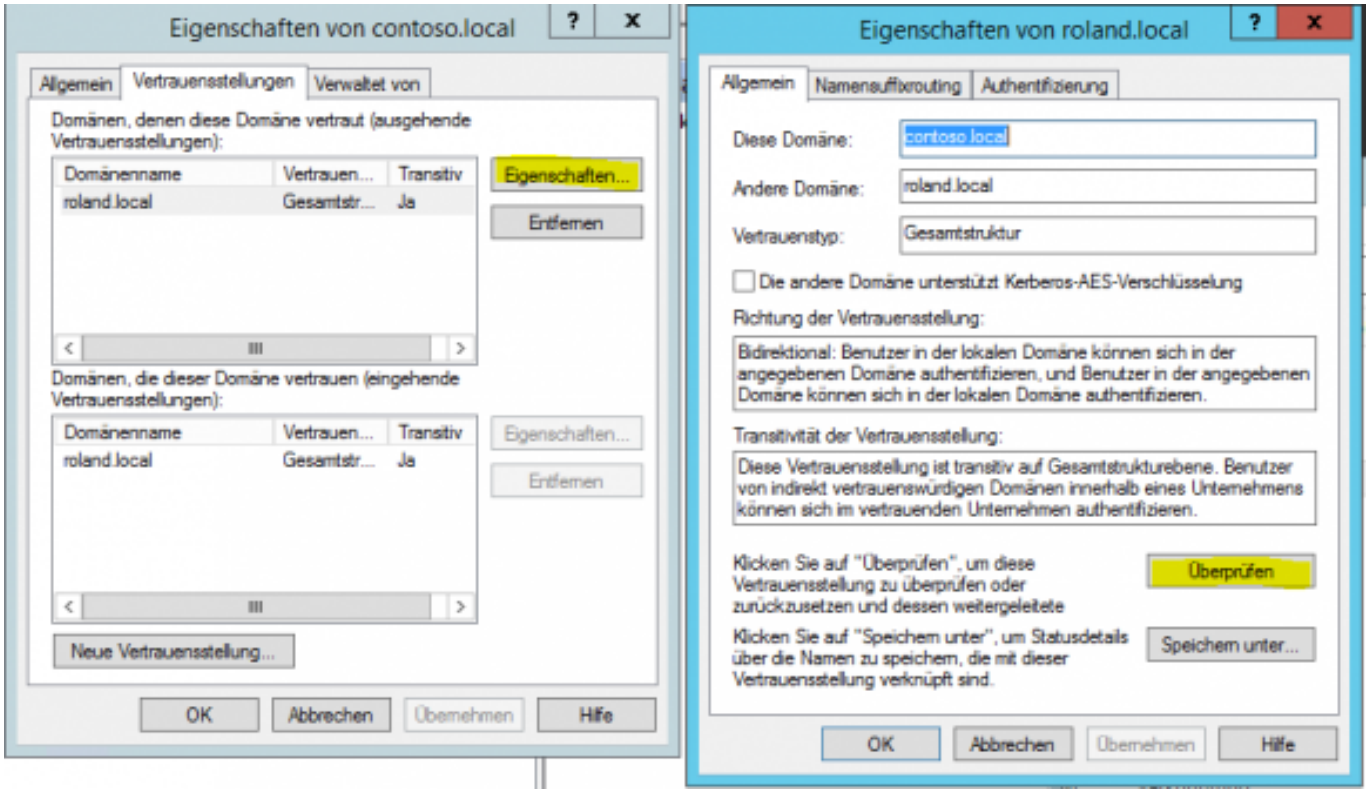
Zuletzt gibt es die Zusammenfassung der bisherigen Konfiguration, die Schaltfläche Weiter führt zu den verbleibenden Schritten.



Ausgehende Vertrauensstellung bestätigen

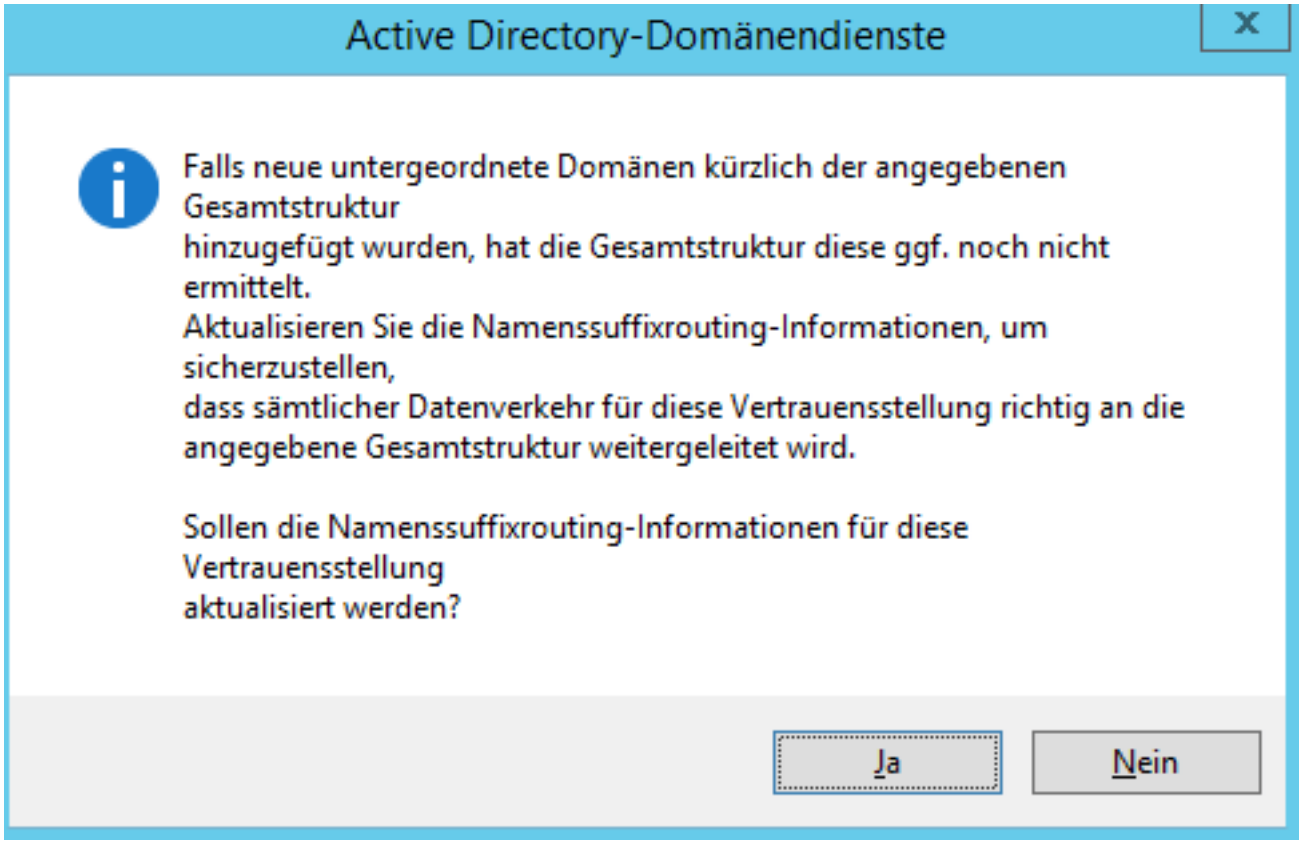
Die Vertrauensstellung sollte auf jeden Fall bestätigt werden, wobei die Bestätigung auch hier für beide Seiten fällig ist. Nach dem Klicken auf Fertig stellen im letzten Dialog wird die Vertrauensstellung auf beiden DCs eingerichtet.

Wir können nun kurz prüfen, ob die Vertrauensstellung richtig funktioniert. Dazu gehe ich auf Eigenschaften und klicke danach auf Überprüfen.



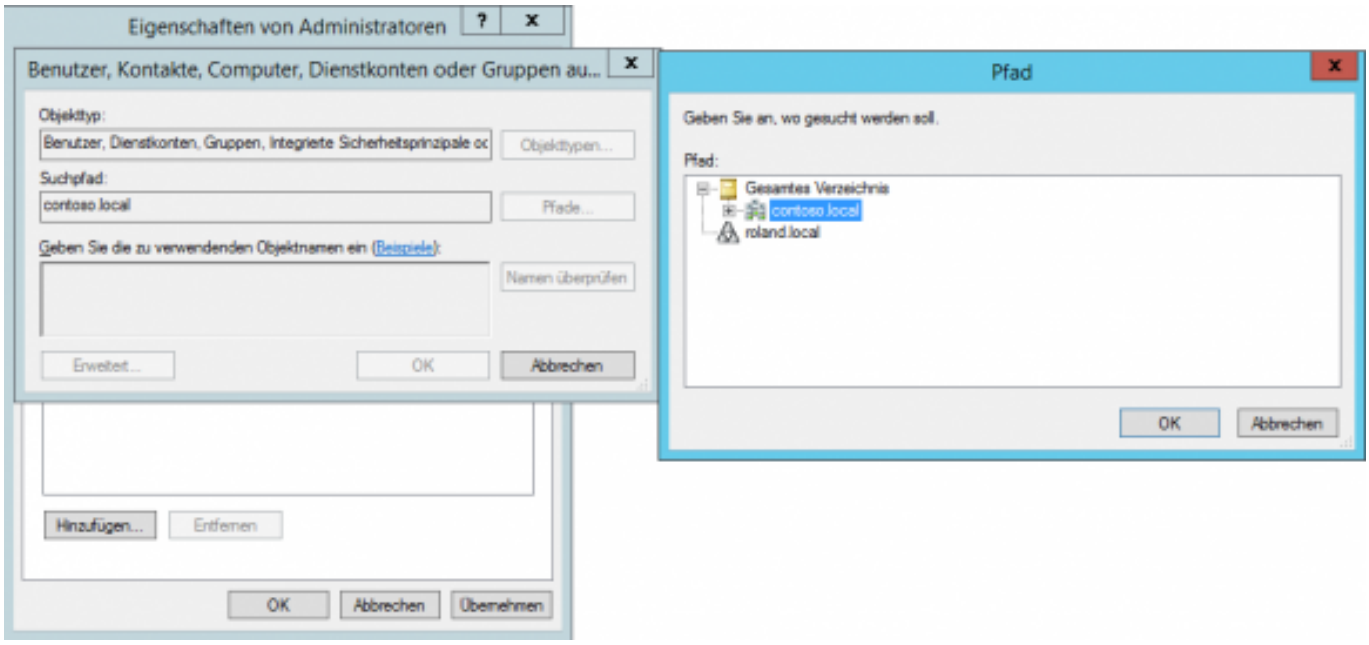
Prüfen, ob die neue Vertrauensstellung funktioniert

Im folgenden Dialog klicken wir auf Ja, um die Informationen für das Routing der Namenssuffixe zu aktualisieren. Die Vertrauensstellung funktioniert soweit.



Informationen für das Routing der Namenssuffixe aktualisieren

Einen weiteren Test liefert das Active Directory mit dem Snapin Active Directory Benutzer und Computer. Hier versuche ich, der Gruppe Administratoren den Administrator aus der anderen Domäne unserer Vertrauensstellung hinzuzufügen.



Die Vertrauensstellung lässt sich testen, indem man den Administator aus der anderen Domäne in die eigene Admin-Gruppe übernimmt

Wir sehen beim Klicken auf Pfade bereits, dass die andere Domäne angezeigt wird und wählen diese aus.

Der Benutzer Administrator wurde gefunden und kann in die Gruppe aufgenommen werden. Damit ist die Konfiguration der Vertrauensstellung soweit abgeschlossen. Für die Migration folgt die Installation und Konfiguration des Active Directory Management Tool (ADMT).

Eindeutige ID: #1090
Verfasser: Hans-Wolfgang Hunsaenger
Letzte Änderung: 2020-07-07 10:43