

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.

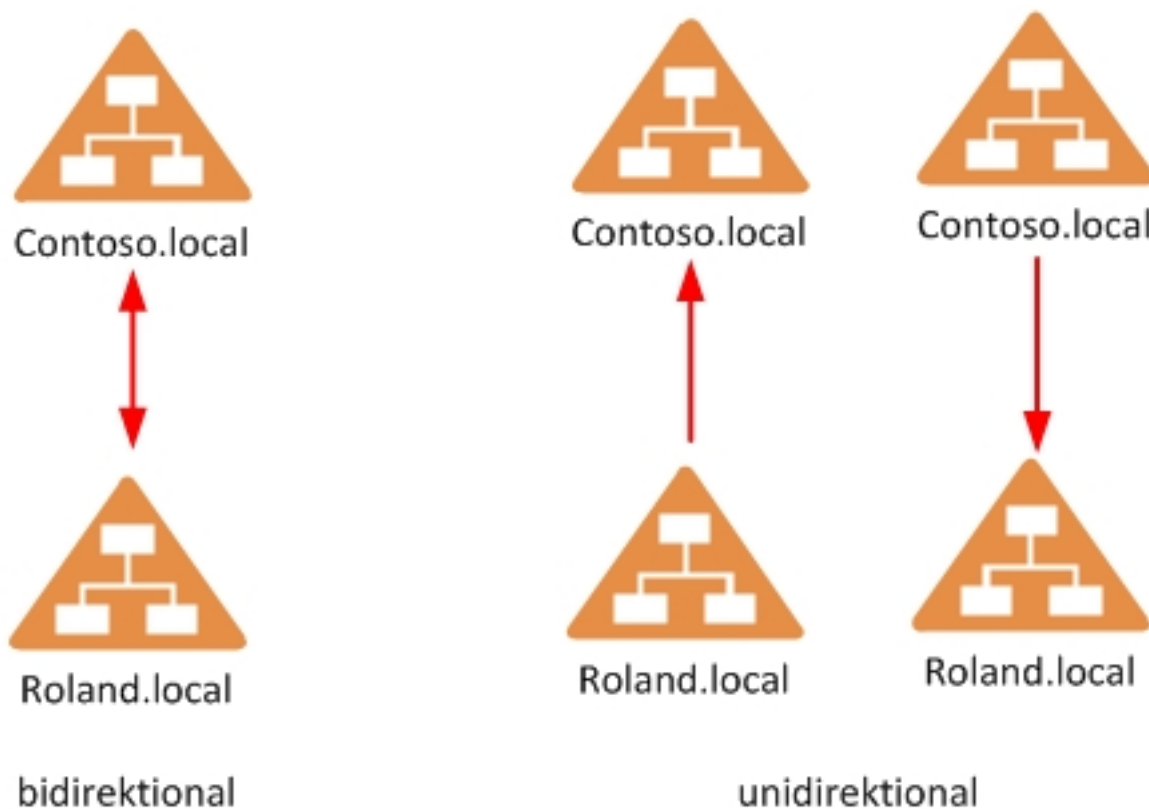
In meinem Beispiel soll eine bestehende Active-Directory-Domäne basierend auf Windows Server 2012 R2 (Contoso.local) auf eine neue Gesamtstruktur migriert werden (Roland.local). Die neue Domäne basiert auf Windows Server 2016.

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

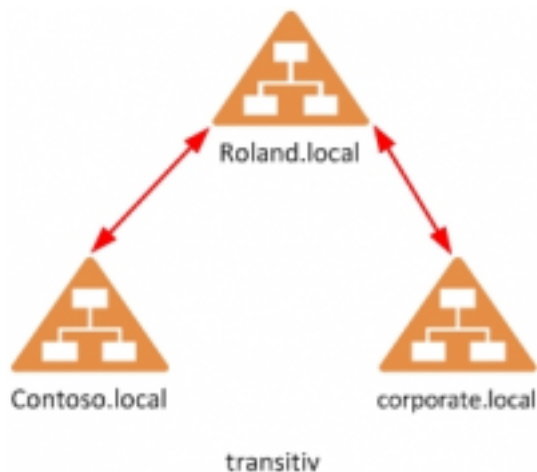
Es gibt im Active Directory zwei Arten von Vertrauensstellungen, die bidirektionale und die unidirektionale:

- Unidirektional ist quasi eine Einbahnstraße. Eine Domäne vertraut 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 Vertrauensstellungen.



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.



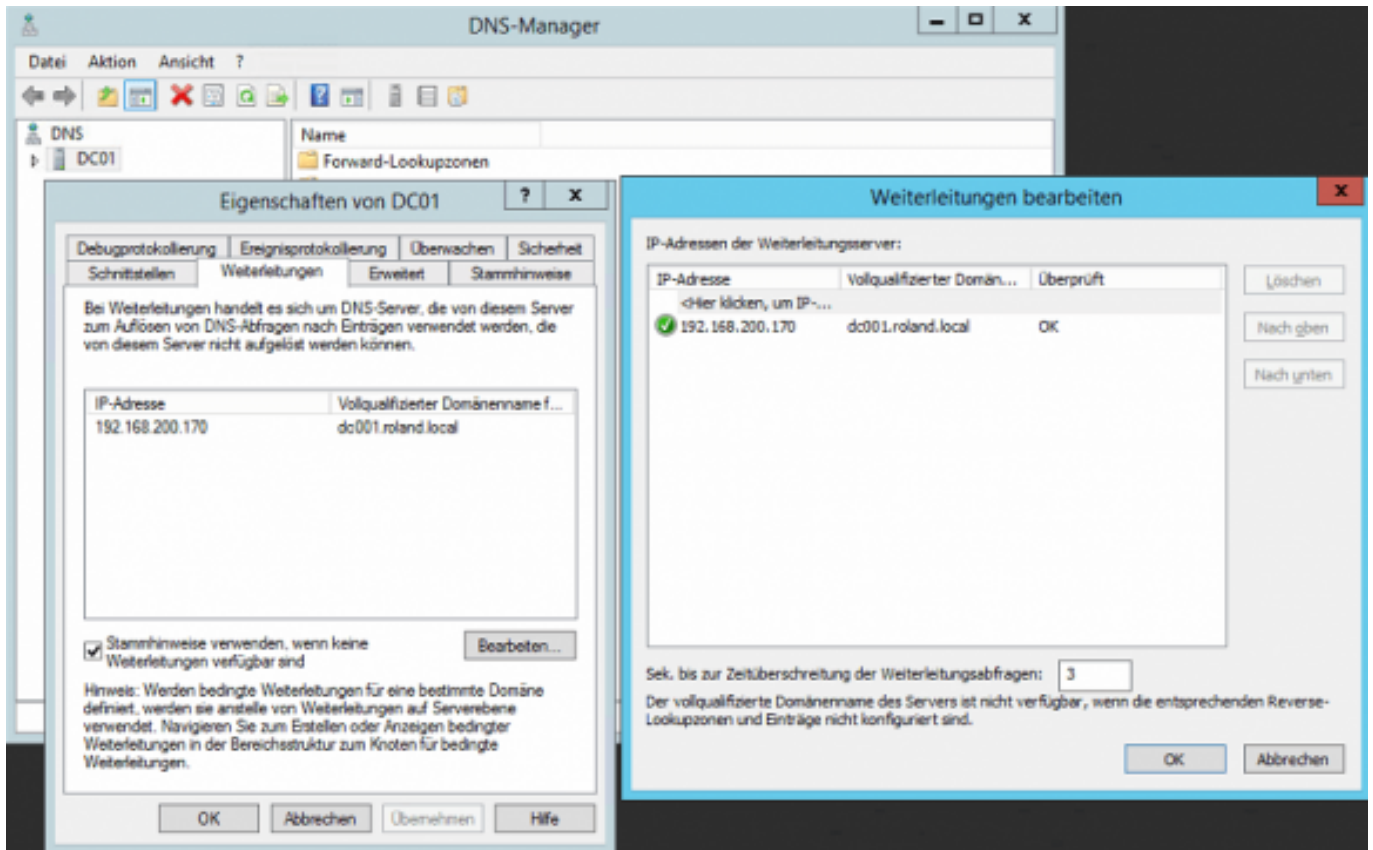
In unserem Beispiel mit den Domänen Contoso.local, Roland.local und Corporate.local würde die Vertrauensstellung von der Domain Contoso.local bis hin zur Domain Corporate.local gehen.

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.

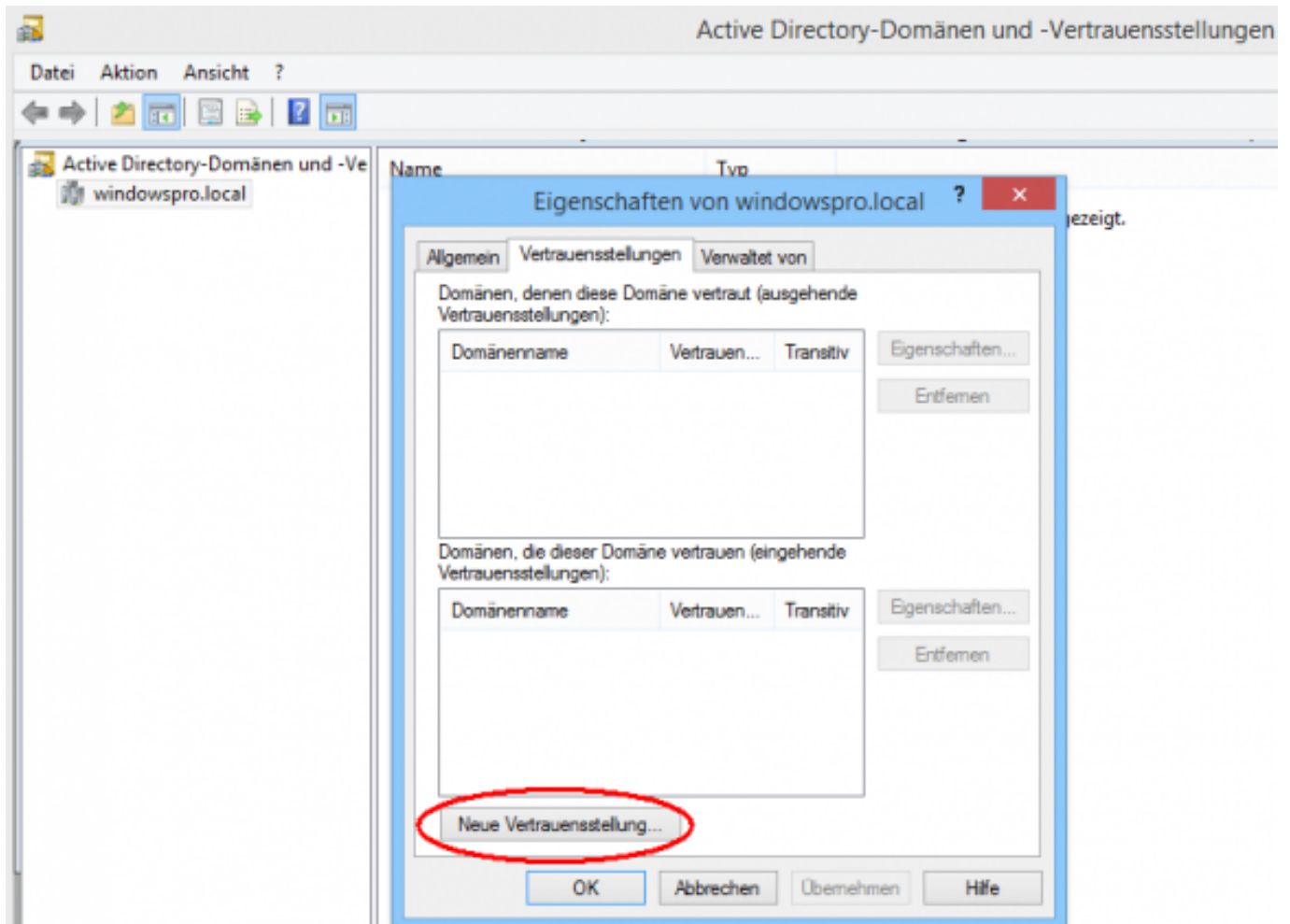
Dafür öffnet man die Eigenschaften der DNS-Server und wechselt zur Registerkarte Weiterleitungen. Die Schaltfläche Bearbeiten startet den Dialog zum Hinzufügen weiterer Name-Server.



DNS-Weiterleitung im MMC-Snapin konfigurieren

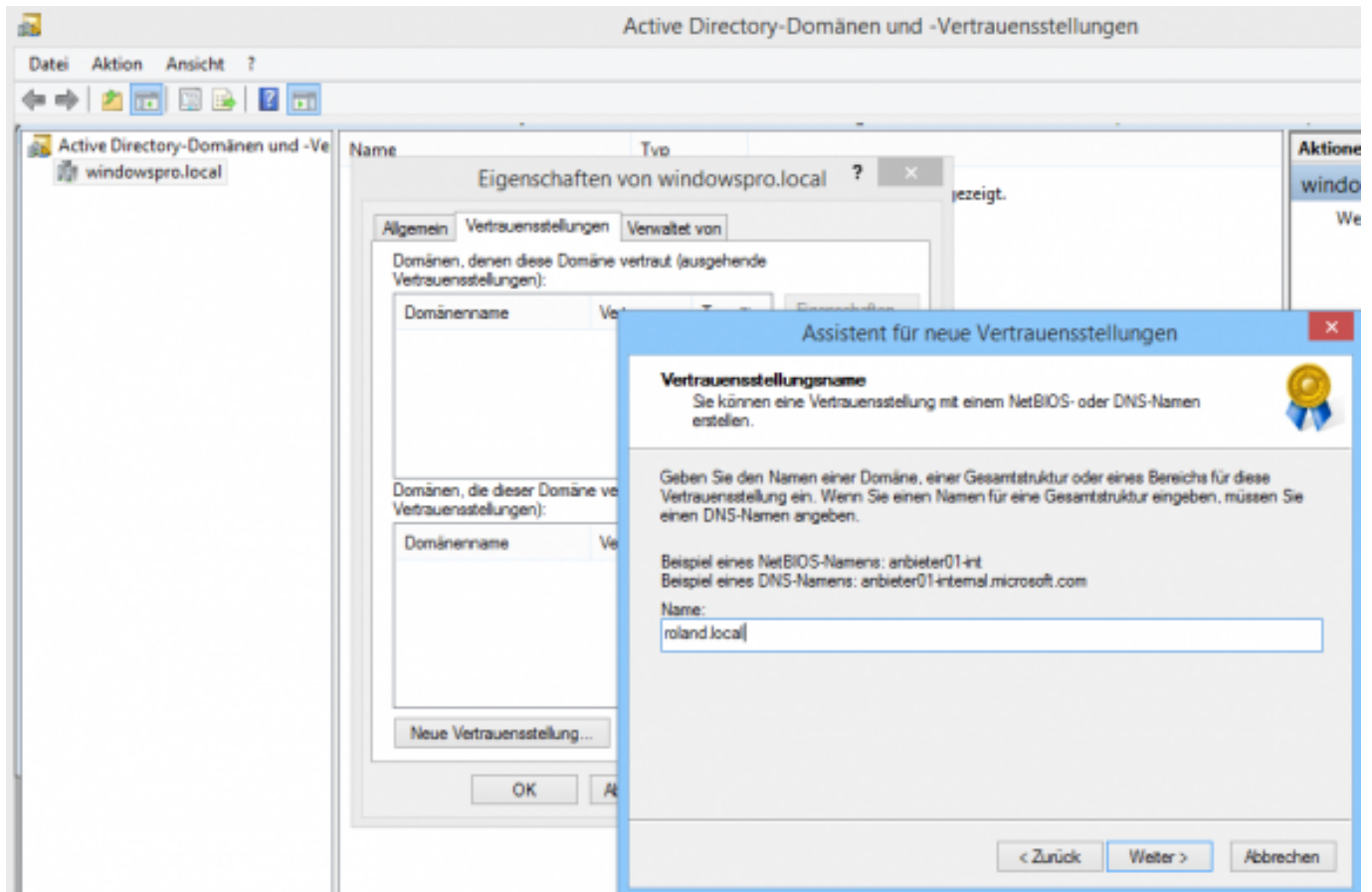
Konfiguration der Vertrauensstellung

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.

Vertrauenstyp

Diese Domäne ist eine Gesamtstrukturdomäne. Sie können eine Gesamtstruktur-Vertrauensstellung erstellen, falls die angegebene Domäne qualifiziert ist.



Wählen Sie den zu erstellenden Vertrauenstyp aus.

- Externe Vertrauensstellung
Eine externe Vertrauensstellung ist eine nicht transitive Vertrauensstellung zwischen einer Domäne und einer anderen, außerhalb der Gesamtstruktur. Eine nicht transitive Vertrauensstellung ist von diesen Domänen abhängig.
- Gesamtstrukturvertrauensstellung
Eine Gesamtstruktur-Vertrauensstellung ist eine transitive Vertrauensstellung zwischen zwei Gesamtstrukturen, die es Benutzern aller Domänen innerhalb einer Gesamtstruktur ermöglicht, in allen Domänen der anderen Gesamtstruktur authentifiziert zu werden.

< Zurück

Weiter >

Abbrechen

Auswahl der Vertrauentyps 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.

Richtung der Vertrauensstellung

Sie können uni- oder bidirektionale Vertrauensstellungen erstellen.



Wählen Sie die Richtung für diese Vertrauensstellung aus.

- Bidirektional**
Benutzer in dieser Domäne können in der angegebenen Domäne, Gesamtstruktur oder dem angegebenen Bereich authentifiziert werden, und Benutzer in der angegebenen Domäne, Gesamtstruktur oder dem angegebenen Bereich können in dieser Domäne authentifiziert werden.
- Unidirektional: eingehend**
Benutzer in dieser Domäne können in der angegebenen Domäne, Gesamtstruktur oder dem angegebenen Bereich authentifiziert werden.
- Unidirektional: ausgehend**
Benutzer in der angegebenen Domäne, Gesamtstruktur oder dem angegebenen Bereich können in dieser Domäne authentifiziert werden.

< Zurück

Weiter >

Abbrechen

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.

Vertrauensstellungsseiten

Sie können die Vertrauensstellungen für beide Domänen erstellen, falls Sie über die entsprechenden Berechtigungen in beiden Domänen verfügen.



Beide Seiten der Vertrauensstellung müssen erstellt werden, damit eine Vertrauensstellung verwendet werden kann. Wenn Sie z. B. eine unidirektionale eingehende Vertrauensstellung in der lokalen Domäne erstellen, muss auch eine unidirektionale ausgehende Vertrauensstellung in der angegebenen Domäne erstellt werden, bevor Authentifizierungsdatenverkehr innerhalb der Vertrauensstellung ausgetauscht werden kann.

Vertrauensstellung für folgende Domänen erstellen:

- Nur für diese Domäne
Diese Option erstellt eine Vertrauensstellung in der lokalen Domäne.
- Für diese Domäne und die angegebene Domäne
Diese Option erstellt Vertrauensstellungen in sowohl der lokalen Domäne als auch den angegebenen Domänen. Sie müssen zum Erstellen von Vertrauensstellungen in der angegebenen Domäne berechtigt sein.

< Zurück

Weiter >

Abbrechen

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.

Assistent für neue Vertrauensstellungen



Benutzername und Kennwort

Sie müssen über Administratorrechte für die angegebene Domäne verfügen, um diese Vertrauensstellung erstellen zu können.



Angegebene Domäne: roland.local

Geben Sie Benutzernamen und Kennwort eines Kontos mit Administratorrechten in der angegebenen Domäne ein.

Benutzername:

 roland\administrator

Kennwort:

●●●●●●●●

< Zurück

Weiter >

Abbrechen

Authentifizierung eines Administrators für das Einrichten einer neuen Vertrauensstellung

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

Authentifizierungsebene für ausgehende Vertrauensstellung–Lokale Gesamtstruktur

Benutzer in der angegebenen Gesamtstruktur können zum Verwenden aller oder nur den von Ihnen angegebenen Ressourcen in der lokalen Gesamtstruktur authentifiziert werden.



Wählen Sie den Authentifizierungsbereich für Benutzer aus Gesamtstruktur "roland.local" aus.

- Gesamtstrukturweite Authentifizierung
Windows authentifiziert Benutzer aus der angegebenen Gesamtstruktur für alle Ressourcen in der lokalen Gesamtstruktur automatisch. Diese Option eignet sich gut, wenn beide Gesamtstrukturen derselben Organisation angehören.
- Ausgewählte Authentifizierung
Windows authentifiziert Benutzer aus der angegebenen Gesamtstruktur nicht automatisch für alle Ressourcen in der lokalen Gesamtstruktur. Nach Fertigstellen dieses Assistenten können Sie individuellen Zugriff für jede Domäne und jeden Server, die bzw. der für Benutzer in der angegebenen Gesamtstruktur zur Verfügung gestellt werden soll, gewähren. Diese Option eignet sich gut, wenn die Gesamtstrukturen zwei verschiedenen Organisationen angehören.

< Zurück

Weiter >

Abbrechen

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

Sie sollten diese Vertrauensstellung erst bestätigen, nachdem die andere Vertrauensstellung erstellt wurde.



Soll die ausgehende Vertrauensstellung bestätigt werden?

- Nein, ausgehende Vertrauensstellung nicht bestätigen
- Ja, ausgehende Vertrauensstellung bestätigen

Klicken Sie auf "Weiter", um die Vertrauensstellung zu bestätigen.

< Zurück

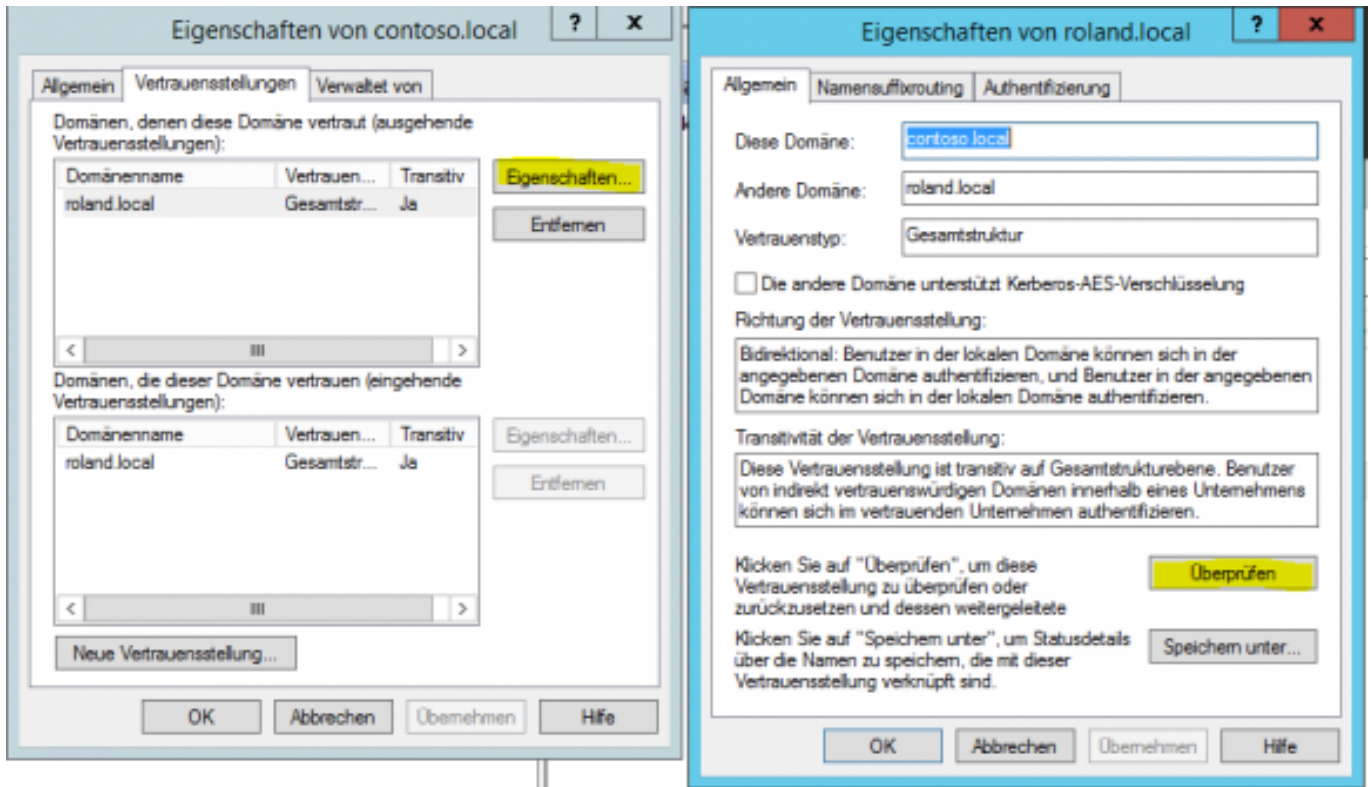
Weiter >

Abbrechen

Ausgehende Vertrauensstellung bestätigen

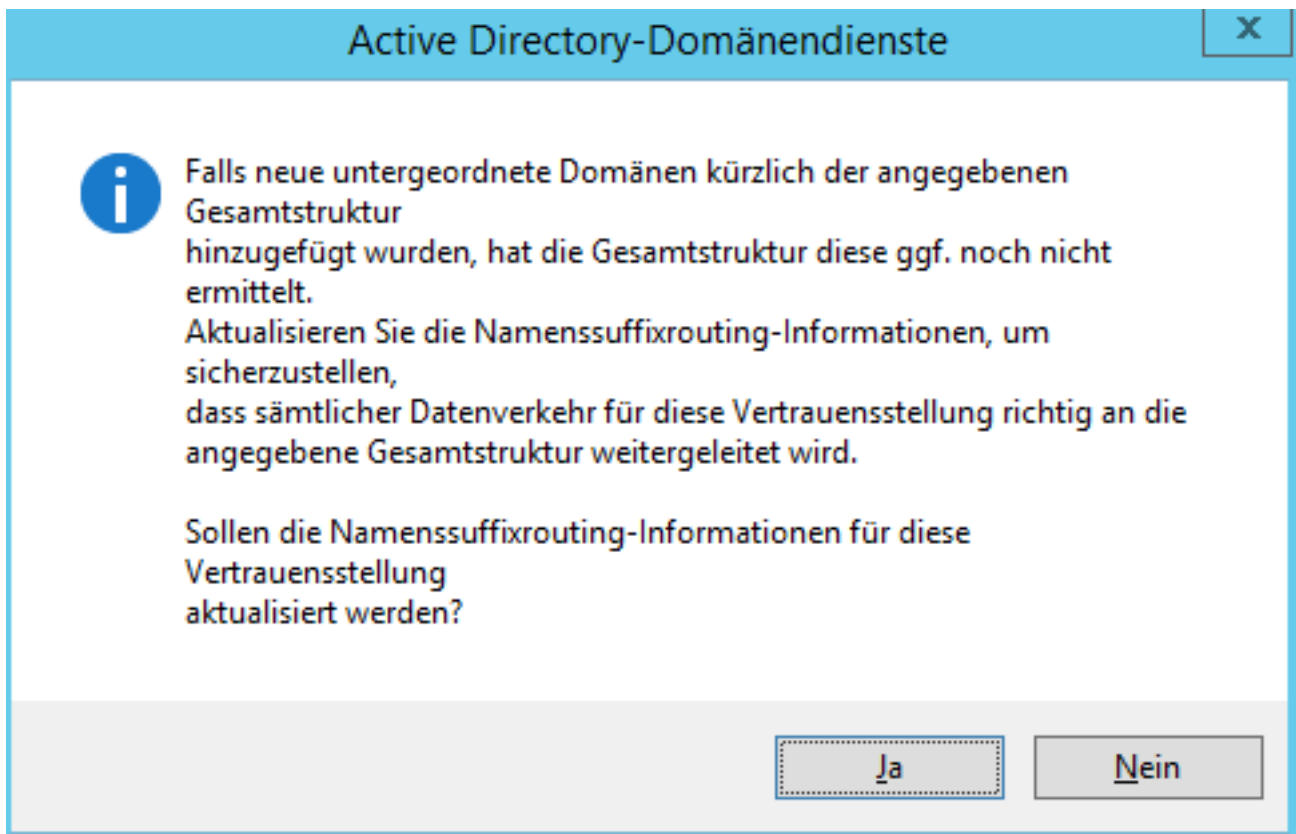
Die Vertrauensstellung sollte auf jeden Fall bestätigt werden, wobei die Bestätigung auch hier für beide Seiten fällig ist. Nach dem Klicken auf Fertig stellen im letzten Dialog wird die Vertrauensstellung auf beiden DCs eingerichtet.

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



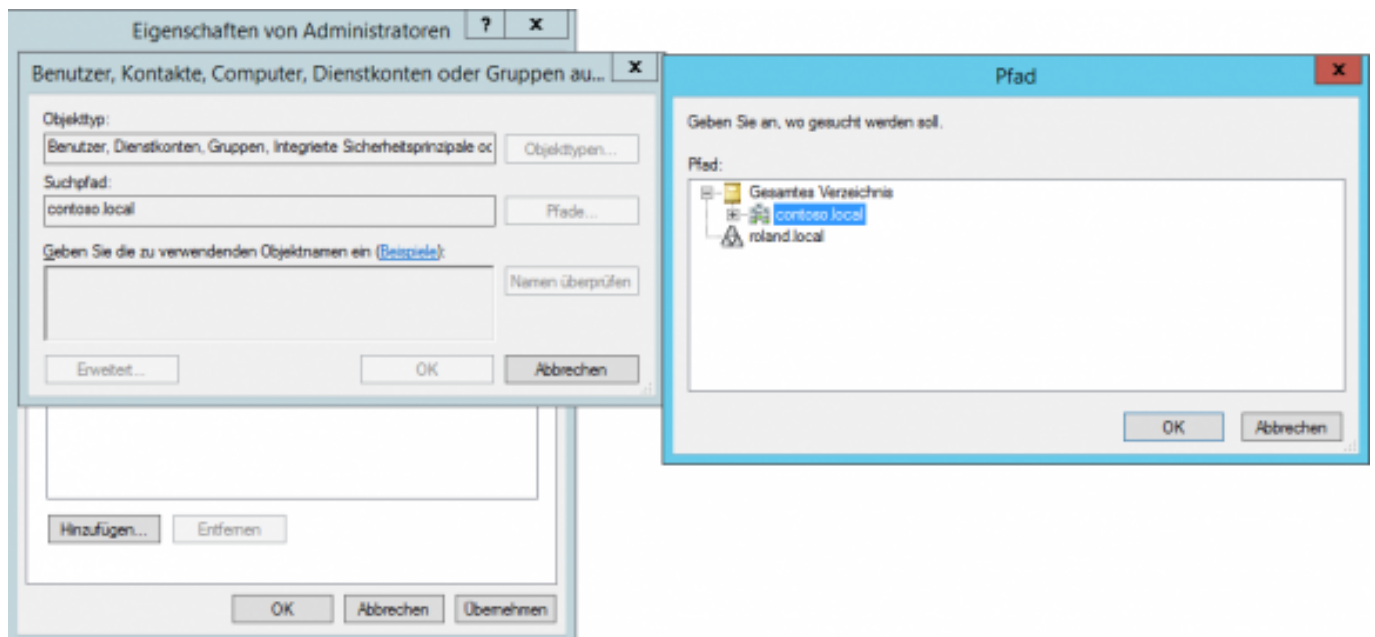
Prüfen, ob die neue Vertrauensstellung funktioniert

Im folgenden Dialog klicken wir auf Ja, um die Informationen für das Routing der Namensuffixe 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 Administrator 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