rendom.exe: Domain Rename
Umbenennen einer Domäne - Schritt für Schritt

Beschreibung des Idealfalls von Mark Heitbrink , CS Result GmbH Regensburg

Dieser Artikel ist im Ablauf an den Step-by-Step Guide von Mohamed Fawzi angelehnt.
http://fawzi.wordpress.com/2008/02/08/domain-rename-procedures/

Microsoft Quellen und Werkzeuge:
Windows Server 2003 Active Directory Domain Rename Tools
http://download.microsoft.com/download/5/6/d/56df978b-9a76-487e-80b7-0250289f2579/domainrename.exe

Understanding How Domain Rename Works
http://download.microsoft.com/download/9/6/5/965e6899-e086-4b3e-8ed6-516ea07ea225/Domain-Rename-Intro.doc

Step-by-Step Guide to Implementing Domain Rename
http://download.microsoft.com/download/c/f/c/cfcbff04-97ca-4fca-9e8c-3a9c90a2a2e2/Domain-Rename-Procedure.doc

Microsoft Exchange Server 2003 Tool zur Korrektur nach Domänenumbenennungen (XDR-Fixup)
http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=24b47d4a-c4b9-4031-b491-29839148a28c

Supplemental steps for using the Exchange Server Domain Rename Fixup tool together with the Windows Server 2003 domain rename tools
http://support.microsoft.com/kb/842116/en-us

Voraussetzungen, Vorbereitungen und/oder auch KO-Kriterien:

- Datensicherung des aktuellen Zustandes ist vorhanden
    - **To do:** **ntbackup** mit **systemstate** auswählen

- Das Domain Rename Tool wird benötigt.
    - **To do:** Download domainrename.exe

- Der Active Directory Forestlevel und damit alle Domainlevel befinden sich im 2003 Native Modus
    - **To do:** Active Directory-Domänen und -Vertrauensstellungen öffnen
        - Name-der-Dom -> Kontext -> Domänenfunktionsebene heraufstufen
        - AD Domänen und Vertrauensstellungen -> Kontext -> Gesamtstrukturfunktionsebene heraufstufen
          Beide Male „Windows Server 2003“ auswählen

- Wenn ein Exchange Server vorhanden ist, dann muss dieser ein Exchange Server 2003 mit mindestens Service Pack 1 sein. Das Tool XDR-Fixup wird benötigt.
    - **To do:** Download XDR-Fixup
    - Ggfs. Service Pack einspielen oder im schlimmsten Fall erst eine Exchange-Migration vornehmen. Das Tool erkennt ältere Exchange Server in der Organisation und bricht den Prozess in so einem Fall ab.

- Der ausführende Benutzer muss Mitglied der Organisations-Admins (Enterprise-Admins) sein.
    - **To do:** Sicherheitsgruppe kontrollieren oder gleich den „richtigen“ Administrator Account verwenden

- Das Tool wird von einer Control Station aus ausgeführt, diese ist ein Mitgliedsserver im AD, ***kein DC***, mit Windows Server 2003. Als Control Station kann der Exchange verwendet werden (wenn er kein DC ist)
    - **To do**: ggfs. Member Server installieren oder eine Virtuelle Maschine verwenden
        - Entpacken der beiden Tools (domainrename.exe + xdr-fixup.exe) nach **c:\rendom** danach sollten sich **gpfixup.exe**, **rendom.exe** und **XDR-Fixup.EXE** darin befinden.
        - Installation der **Windows Support Tools** (suptools.msi) von der Installations CD. *Ich persönlich kopiere die Tools nach Installation immer nach %systemroot%\system32, da sie dann direkt über die PATH Variable gefunden werden. Vorhandene Dateien bitte NICHT ersetzen.*

- Im DNS muss die neue Zone mit dem Speicherort der SRV Records vorhanden sein.
    - **To do:**
        - DNS Verwaltung öffnen und eine neue Zone erstellen (AD integriert) **„NeuerName.derdom“**
        - Ebenfalls eine neue Zone für die SRV Records erstellen (AD integriert) **„_msdcs.NeuerName.derdom“**
          In beiden Zonen „Sichere und unsichere Updates zulassen“

- Das neue DNS Suffix sollte im Active Directory als erlaubte Endung für die Hostnamen eingetragen werden, Manipulation des Attributs: **msDS-AllowedDNSSuffix**
    - **To do:** adsiedit.msc öffnen
        - Domain -> "DC=AlterName,DC=derdom" -> Kontext -> Eigenschaften -> Attribut Editor -> **msDS-AllowedDNSSuffix = NeuerName.derdom**

- Alle aktuell unbeteiligten System sollten heruntergefahren werden, nur die DCs, der/die Exchange Server und die Control Station laufen weiter.
    - **To do:** Rechner herunterfahren

- Die Zertifikatsdienste sind auf ***keinem*** DC installiert.
    - **To do:** wenn die CA auf einem DC liegt: "How to move a certification authority to another server"

- Alle Server die DFS bereitstellen sind mindestens Windows 2000 mit Service Pack 3
    - **To do:** ggfs. Updates und Service Packs einspielen

- **Datensicherung des aktuellen Zustandes ist vorhanden**
    - **To do:** **ntbackup** mit **systemstate** auswählen

Ausnahmen und Sonderfälle, die in dieser Anleitung nicht abgebildet sind, da wir den Idealfall beschreiben:

- Das Active Directory hat keine Subdomänen.
- Es sind keine Vertrauensstellungen vorhanden.
- Es sind keine Zertifikatsdienste installiert
- Serverbasierte Profile sind nicht auf einem DFS hinterlegt
- Die Ordnerumleitung für div. Ordner des Profils zeigen nicht auf einen DFS Stamm
- An den Computers wurden keine DNS Suffixe manuell oder per Gruppenrichtlinie definiert
- Der Exchange Server läuft nicht auf einem Cluster

Für diese Fälle verweise ich auf das Step-by-Step Guide to Implementing Domain Rename
In dem Dokument sind diese Fälle und natürlich auch der Idealzustand genau beschrieben und die Anleitungen mit weiterführenden Lösungen enthalten.

Zu jedem der folgenden Schritte findet man im Step-by-Step Guide to Implementing Domain Rename Troubleshooting Tips, falls es zu Fehlermeldungen kommt.

Schritt für Schritt:

1. Voraussetzungen, Vorbereitungen und/oder auch KO-Kriterien erneut durchlesen und die Systeme entsprechend vorbereiten

2. An der Control Station eine Eingabeaufforderung öffnen und nach **c:\rendom** wechseln und eine aktuelle Liste der Domänennamen und Struktur erstellen. Es wird über den Befehl automatisch eine XML Datei „**Domainlist.xml**“ im aktuellen Verzeichnis erstellt.

   rendom.exe /list

3. Sicherheitskopie der **Domainlist.xml** erstellen, sie wird hinterher auch noch für das XDR-fixup zum Vergleich benötigt und natürlich für einen möglichen Restore.

   copy domainlist.xml domainlist-save.xml

4. Öffnen der **Domainlist.xml** mit einem Editor und Anpassung der Namen. Blau/fett markierte Zeilen über suchen/ersetzen mit dem neuen Namen anpassen. Diese finden in folgenden Tags statt:

   3x in <DNSname> … </DNSname>
   1x in <NetBiosName> … </NetBiosName>

```
<?xml version ="1.0"?>
<Forest>
        <Domain>
                <!-- PartitionType:Application -->
                <Guid>d2b9045f-5819-4f6c-90ed-00427654250d</Guid>
                <DNSname>DomainDnsZones. NeuerName.derdom </DNSname>
                <NetBiosName></NetBiosName>
                <DcName></DcName>
        </Domain>
        <Domain>
                <!-- PartitionType:Application -->
                <Guid>31827903-2b2f-481e-9091-7be98f21d9e1</Guid>
                <DNSname>ForestDnsZones. NeuerName.derdom </DNSname>
                <NetBiosName></NetBiosName>
                <DcName></DcName>
        </Domain>
        <Domain>
                <!-- ForestRoot -->
                <Guid>44ae11c6-4d2b-4a16-b6af-ee8e26d6f194</Guid>
```

```
                <DNSname> NeuerName.derdom </DNSname>
                <NetBiosName> NeuerName</NetBiosName>
                <DcName></DcName>
        </Domain>
</Forest>
```

5. Kontrolle und Abgleich, ob die neue XML Datei dem Wunsch entspricht. Ebenfalls wird die Syntax des XML Schemas überprüft und damit sichergestellt, daß die Konfigurationsdatei überhaupt verwendet werden kann.

rendom /showforest

```
NeuerName.derdom  [ForestRoot Domain, FlatName:NEUERNAME]
DomainDnsZones.NeuerName.derdom  [PartitionType:Application]
ForestDnsZones.NeuerName.derdom  [PartitionType:Application]
The operation completed successfully.
```

6. Hochladen der Konfiguration ins AD. Es werden 2 Dateien erstellt:
DcList.xml und **DNSRecords.txt**
In der **DcList.xml** sind zum einen die Instruktionen für die Umbenennung enthalten, aber auch der aktuelle Status des Vorgangs für jeden DC separat.

rendom /upload

Inhalt der **DcList.xml**:

```
<?xml version ="1.0"?>
<DcList>
        <Hash>YeXZIXeAutaEiCKvOSOJlYkVfBI=</Hash>
        <Signature>7zi3p+bjKw+w63w27ydH7X6SUQA=</Signature>
        <DC>
                <Name>DC01.AlterName.derdom</Name>
                <State>Initial</State>
                <Password></Password>
                <LastError>0</LastError>
                <LastErrorMsg></LastErrorMsg>
                <FatalErrorMsg></FatalErrorMsg>
                <Retry></Retry>
        </DC>
</DcList>
```

7. Wir suchen uns den FSMO Inhaber der Rolle **Domain Naming Master** und „pushen“ die Replikation.

   a.) **dsquery server -forest -hasfsmo name**

   b.) **repadmin /syncall /d /e /P /q NameNamingMaster**
   (Achtung case-sensitiver Befehl)

8. Vor der eigentlichen Durchführung muss sichergestellt sein, dass alle DC den Status von „Initial“ auf **<State>Prepared</State>** umgesetzt haben und damit die Replikation aus dem vorherigen Schritt erfolgt ist. Status Kontrolle in der **DcList.xml** nach folgendem Aufruf:

   rendom /prepare

   Waiting for DCs to reply.
   Waiting for DCs to reply.
   DC01.AlterName.derdom was prepared successfully
   1 server contacted, 0 servers returned Errors
   The operation completed successfully.

9. Sobald jeder DC Erfolg gemeldet hat kommt die eigentliche Ausführung.

   rendom /execute

   Waiting for DCs to reply.
   Waiting for DCs to reply.
   The script was executed successfully on DC01.AlterName.derdom
   1 server contacted, 0 servers returned Errors
   The operation completed successfully.

   Der Status in der **DcList.xml** wechselt erneut : **<State>Done</State>**

10. Kümmern wir und jetzt um Exchange, wer keinen Exchange hat kann diesen Punkt natürlich überspringen. Wir geben dem Befehl den Ausgangspunkt (/s:domainlist-save.xml) und die neue Struktur (/e:domainlist.xml) mit. Die durchzuführenden Änderungen werden erstellt (/changes:changescript.ldf) und wir sichern uns die Möglichkeit zum Restore (/restore:restorescript.ldf)

    XDR-Fixup.exe /s:domainlist-save.xml /e:domainlist.xml /changes:changescript.ldf /restore:restorescript.ldf

    Fixed 13 objects.

The operation completed successfully.

Beispiel Eintrag aus der **changes.ldf**

dn: CN=Public,CN=1,CN=HTTP,CN=Protocols,CN= EX01,CN=Servers,CN=Erste administrative Gruppe,CN=Administrative Groups,CN=Erste Organisation,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=neuername,DC=derdom
changetype: modify
delete: msExchBasicAuthenticationDomain
msExchBasicAuthenticationDomain: alternname.derdom
-
add: msExchBasicAuthenticationDomain
msExchBasicAuthenticationDomain: neuername.derdom

Mit der **changes.ldf** importieren wir die neuen Namen für die Exchange Attribute im AD.

11. **2-maliger** Neustart der Control Station. Wenn es der Exchange Server ist kann man diesen Punkt überspringen und den Punkt 12. ausführen.
    Nach erfolgreichem 2ten Neustart wird schon **„NeuerName“** in der Anmeldeliste angezeigt.

    shutdown –r –t 0

12. Import der neuen Exchange Attribute

    ldifde -i -f changescript.ldf
    Verbindung mit "DC01.alternname.derdom" wird hergestellt.
    Anmelden als aktueller Benutzer unter Verwendung von SSPI
    Das Verzeichnis wird aus der Datei "changescript.ldf" importiert.
    Die Einträge werden geladen.....
    13 Einträge wurden erfolgreich geändert.
    Der Befehl wurde einwandfrei durchgeführt.

13. **2-maliger** Neustart des Exchange Servers

    shutdown –r –t 0

14. Wir beenden das Domain Rename

    rendom.exe /end

15. Jetzt werden die Verlinkungen zu den Default Richtlinien korrigiert, die im Gegensatz zu den selbsterstellten HardCodiert sind. Es muss jeweils der Alte/Neue DNS Name und Alte/Neue

NetBIOS Name angegeben werden unter Verwendung des PDC Emulators (letzterer empfohlen)

gpfixup /olddns:alternname.derdom /newdns:neuername.derdom /oldnb:Alternname /newnb:Neuername /dc:DC01.Alternname.derdom

Group Policy fix up utility Version 1.1 (Microsoft)
Start fixing group policy (GroupPolicyContainer) objects:
.....
Start fixing site group policy links:
.
Start fixing non-site group policy links:
.....
gpfixup tool executed with success.

16. **2-maliger** Neustart **ALLER!** Systeme: Domain Controllers, Workstation, MemberServer etc. Einige Workstations werden Fehler melden und sich nicht in automatisch in die Neue Namengebung einfügen. Aber diese Problemfälle sind leicht zu beheben:

    Workstation in eine Workgroup stellen und nach Neustart zurück ins AD

    P.S.: Ein Königreich für ein funktionelles Wake-On-Lan, z.B.: Special Operations - GPUpdate
    http://www.specopssoft.com/products/specopsgpupdate/default.asp

17. Grundsätzlich betrachtet sind wir mit dem Prozess des Umbenennens fertig. Jetzt folgen die anstehenden Aufräumarbeiten und weitere manuelle Anpassungen.

    rendom /clean

Aufräum- und Nacharbeiten

18. Im Gegensatz zu den Clients und Memberservern, deren Hostname sich automatisch geändert hat, geschieht der folgende Schritt an **JEDEM DC** per Hand. Wir fügen einen zusätzlichen Namen hinzu, machen diesen zum ersten und löschen dann nach Neustart den alten. Die **netdom.exe** ist in den **Windows Support Tools** enthalten

    a) **netdom computername DC01.AlterName.derdom /add:DC01.NeuerName.derdom**
    b) **netdom computername DC01.AlterName.derdom /makeprimary:DC01.NeuerName.derdom**
    c) **shutdown –r –t 0**

19. Jetzt wird der alte Name gelöscht

netdom computername DC01.NeuerName.derdom /remove: DC01.AlterName.derdom

20. Auf dem Exchange sollte die **Empfängerrichtlinie** angepasst werden, wenn sich durch die Domänen Namensänderung auch diese geändert haben. Dieser Punkt ist weiniger interessant, wenn man vor der Umstellung Intern schon einen von der externen/öffentlichen Maildomain unterschiedlichen Namen verwendet hat und die Empfängerrichtlinie schon darauf angepasst wurde.

21. Exchange: Der angegebene Domänen Controller Recipient Update Service muss per Hand umgestellt werden

Exchange-System Manager -> Empfänger -> Empfängeraktualisierungsdienste -> Auf allen Einträgen -> Eigenschaften -> Reiter Allgemein ->
Windows Domänen Controller = DC01.NeuerName.derdom

22. DNS aufräumen.

- **a.** Die beiden alten Zonen löschen:
  AlterName.derdom
  _msdcs.Alternname.derdom
- b. Alle Einträge in den neuen Zonen durchschauen, ob noch der alte Name oder DomänenName auftaucht, z.B.: im SOA Eintrag steht noch
  „hostmaster.Alternname.derdom“ -> „hostmaster.NeuerName.derdom“

23. Erneuter Start mindestens eines DCs und des Exchange mit anschließender Kontrolle der Ereignisanzeige.

24. Abschluss Kontrolle von XDR-Fixup, bei folgendem Fehler sollte man tatsächlich beachten, was da steht.

XDR-Fixup /verify:restorescript.ldf /changes:verifycorrections.ldf

It appears that the server alternname.derdom has a static DNS entry and was not renamed to neuername.derdom. An LDIF transaction has been written to RESTORESCRIPT.LDF to correct this situation. **If this warning is wrong, please check that the server has been rebooted twice and wait for the DCs to replicate**
Verified that the server Ex01.alternamederdom was renamed to EX01.neuername.derdom
Verify pass has completed