POGLAVLJE 1

# Napredna infrastruktura aktivnih direktorijuma

Ukoliko ste administrator u nekom srednjem ili većem preduzeću, verovatno ste zaduženi za upravljanje većim brojem domena, možda čak i većim brojem šuma, a ne za upravljanje šumom sa samo jednim domenom. U ovom poglavlju saznaćete kako i zašto bi trebalo da konfigurišete šume sa većim brojem domena stabla i prednosti koje nude pojedini funkcionalni nivoi. Takođe, naučićete kako da konfigurišete različite vrste odnosa poverenja i da njima upravljate kako biste korisnicima iz jedne šume ili iz jednog domena dozvolili odgovarajući pristup resursima u drugoj šumi, drugom domenu ili Kerberos oblastima.

### Lekcije u ovom poglavlju:

- Lekcija 1: Konfigurisanje domena i šuma
- Lekcija 2: Konfigurisanje poverenja

## Pre nego što počnete

Da biste obavili praktična vežbanja iz ovog poglavlja potrebno je da već imate računare SYD-DC, MEL-DC, CBR-DC i ADL-DC instalirane onako kako je to opisano u uvodu, korišćenjem probne verzije Windows Servera 2012.

## Lekcija 1: Konfigurisanje domena i šuma

Kao iskusan administrator već ste verovatno dobro upoznati sa konfiguracijom šuma aktivnog direktorijuma sa jednim domenom. U ovoj lekciji, naučićete nešto više o okruženjima sa više domena i više šuma. Otkrićete kako da nadogradite postojeći domen i šumu tako da oni koriste samo Windows Server 2012 kontrolere domena, a saznaćete i to kako da konfigurišete UPN sufikse.

**Posle ove lekcije:**

- bolje ćete razumeti okruženje aktivnog direktorijuma sa više domena
- bolje ćete razumeti okruženje aktivnog direktorijuma sa više šuma
- moći ćete da nadogradite postojeće domene i šume
- moći ćete da konfigurišete višestruke sufikse osnovnog korisničkog imena (UPN – User Principal Name)

**Očekivano trajanje lekcije: 45 minuta**

## Okruženje aktivnog direktorijuma sa više domena

Većina postojećih postavki aktivnog direktorijuma u manjim preduzećima i preduzećima srednje veličine ima jedan domen. To nije oduvek bilo tako pošto su ranije verzije Windows Server operativnog sistema, kao što je Windows NT4, podržavale samo manji broj korisničkih naloga. Podrška za manji broj naloga obično je iziskivala korišćenje više domena, pa nije bilo neuobičajeno da se vide organizacije srednje veličine koje koriste veoma složenu strukturu domena.

Svaki kontroler domena iz Windows Servera 2012 može da stvori približno 2,15 milijardi objekata tokom svog veka trajanja, a svaki domen podržava stvaranje približno 2,15 milijardi relativnih identifikatora (RID – relative identifier). Uzimajući u obzir ove cifre, samo mali broj administratora primenjuje šume sa više domena, jer im je to potrebno da bi ostvarili podršku za veći broj korisnika. Naravno, u veoma velikim organizacijama, opterećenje zbog replikacije između čvorišta može da dovede u pitanje održavanje domena sa nekoliko hiljada korisničkih naloga, pa se pitanjima čvorišta i replikacije između njih bavimo u poglavlju 2 „Čvorišta i replikacija aktivnog direktorijuma".

Postoji više razloga zbog kojih organizacije primenjuju šume sa više domena. Neki od tih razloga su:

- **Nasleđena struktura domena** Bez obzira na to što novije verzije Windows Server operativnog sistema upravljaju velikim brojem objekata veoma efikasno, neke organizacije zadržale su strukturu domena koja je uspostavljena onda kada su prvi put usvojili aktivni direktorijum.
- **Organizacioni ili politički razlozi** Neke organizacije su izuzetno složene i mogu se sastojati iz zasebnih kompanija koje imaju zajedničko administrativno i upravljačko jezgro. Primer za to su fakulteti na univerzitetima u Evropi ili Australiji, kao što je Fakultet prirodnih nauka, koje sačinjavaju različiti odseci ili škole, kao što su škola za fiziku i odsek za botaniku. Iz političkih ili organizacionih razloga odlučeno je da svaki odsek ili škola

imaju sopstvene domene koji su deo sveukupne šume domena fakulteta. Aktivni direktorijumi omogućavaju da organizacije prave prostore imena koji ispunjavaju njihove potrebe, bez obzira na to što se te potrebe možda ne preslikavaju baš najbolje na ispunjenje ciljeva gledano sa strogo tehničkog stanovišta.

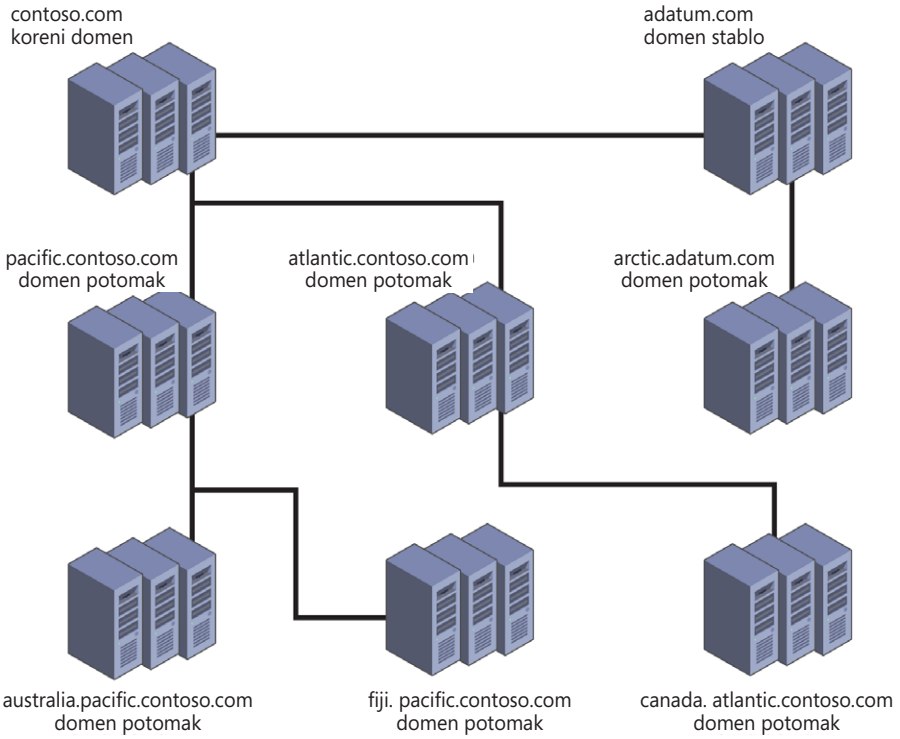
- **Bezbednosni razlozi** Domeni omogućavaju da pravite bezbednosna razgraničenja tako da imate skup administratora koji mogu da upravljaju računarima i korisnicima u svom domenu, ali koji ne mogu da upravljaju računarima i korisnicima u zasebnom domenu. Mada je sličan cilj moguće postići delegiranjem privilegija, većina organizacija više voli da koristi zasebne domene kako bi postigle ovaj cilj.

***U PRAKSI*** **PRIMAT POLITIKE NAD TEHNOLOGIJOM**

Veoma je važno da se razume da tehnički zaluđenici često smatraju tehnologiju nečim što je potpuno razdvojeno od organizacione politike, pri čemu su najumešnija tehnička rešenja istovremeno i najbolja, što ne znači da i svi drugi uvek dele takvo gledište. Dok sam radio kao sistem administrator na Australijskom Univerzitetu, postojala je zajednička prostorija u jednoj od zgrada u kojoj su se nalazila dva različita štampača koje su koristili različiti odseci, bez obzira na to što su ta dva odseka bila deo istog fakulteta. Zaposleni u oba odseka bili su uvereni u to da bi štampače na mreži trebalo obeležiti tako da se štampači prepoznaju po odsecima i da korisnici iz jednog odseka ne bi, ni u kom slučaju, trebalo da štampaju na štampaču koji pripada drugom odseku. Mada spletkarenja između odseka baš mnogo i ne zanimaju zaluđenike iz odseka za informacione tehnologije (IT), administratorima koji ne vode računa o ne uvek jasno utvrđenim razgraničenjima to se obično obija o glavu.

## Domen stablo

Domen stablo je skup imena kojima je zajedničko ime *korenog domena*. Na primer, contoso.com može da ima domene pacific.contoso.com i atlantic.contoso.com kao domene potomke (child domain), a i ti domeni mogu da imaju svoje domene potomke. Šuma domena može da ima više *domena stabla*. Kada pravite novo stablo u šumi, koren tog novog stabla je *domen potomak* prvobitnog korenog domena. Na slici 1-1, domen adatum.com je koren novog domena stabla u contoso.com šumi.




**SLIKA 1-1** Contoso.com kao koreni domen u šumi od dva stabla

Dubina domena stabla ograničena je najvećom dužinom punog imena domena (FQDN – fully qualified domain name) za matični računar od 64 znaka. To znači da ime matičnog računara i ime domena zajedno ne smeju da budu duži od 64 znaka, uključujući i tačke koje razdvajaju sve delove imena. Na primer, ime 3rd-floor-printer (za štampač na trećem spratu) ne bi moglo da se koristi na domenu melbourne.victoria.australia.pacific.contoso.com pošto se ne može iskoristiti kao ime matičnog računara u šumi aktivnog direktorijuma pošto ime matičnog računara premašuje ograničenje od 64 znaka.

## Provera autentičnosti unutar šume

Svi domeni unutar iste šume automatski dele poverenje između sebe. To znači da u okruženju prikazanom na slici 1-1, korisniku u domenu australia.pacific.contoso.com možete dodeliti ovlašćenja za resurse u domenu arctic.adatum.com pri čemu ne morate da bilo šta dodatno konfigurišete.

Zbog automatski ugrađenih odnosa poverenja, primena šume sa jednim domenom nije pogodna za nezavisne organizacije, čak i ako one međusobno sarađuju. Šuma sa jednim domenom omogućava da jedan korisnik ili više njih steknu administrativnu kontrolu nad njom. Većini organizacija ne prija to da neko drugi pa čak ni partneri u koje imaju poverenja stekne administrativnu kontrolu nad njihovim IT okruženjem. Kada bude bilo potrebno da korisnicima iz partnerske organizacije dopustite pristup resursima, to možete da uradite konfigurisanjem odnosa poverenja ili saveza. O odnosima poverenja više možete pročitati u lekciji 2 iz ovog poglavlja, a o savezima u poglavlju 10 „Savezi servisa aktivnog direktorijuma“.

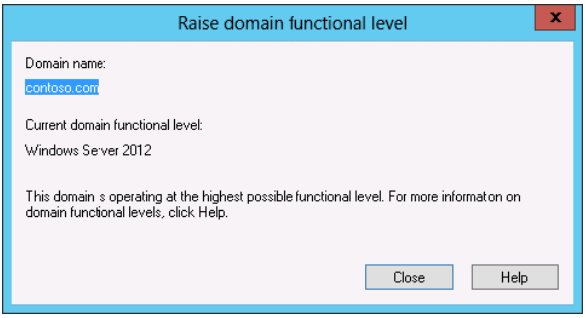
## Funkcionalni nivoi domena

Funkcionalni nivoi domena određuju funkcionalnost aktivnog direktorijuma i mogućnosti koje stoje na raspolaganju. Što je *funkcionalni nivo domena* viši, to na raspolaganju stoji više funkcionalnosti i veće mogućnosti. Kontrolere domena Windows Servera 2012 možete koristiti sa sledećim funkcionalnim nivoima domena:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

Ograničavajući faktor za funkcionalni nivo domena je kontroler domena koji se koristi kao matični računar za aktivni direktorijum. Ukoliko vaša organizacija ima Windows Server 2003 kontrolere domena, ne možete da podignete funkcionalni nivo sve dok ne zamenite ili nadogradite te kontolere domena na najnoviju verziju Windows Server operativnog sistema.

Funkcionalne nivoe domena možete da menjate korišćenjem konzole Active Directory Users and Computers, konzole Active Directory Domains and Trusts kao što je prikazano na slici 1-2 ili komandom Set-ADDomainMode Windows u komandnom prozoru PowerShell. Da biste to obavili, potrebno je da koristite nalog koji je član grupa Domain Admins ili Enterprise Admins.




**SLIKA 1-2** Podizanje ili potvrđivanje funkcionalnog nivoa domena

### Funkcionalni nivo Windows Servera 2003

Funkcionalni nivo domena Windows Servera 2003 je najniži nivo na koji možete da uvedete kontrolere domena koje pokreće operativni sistem Windows Server 2012. Ovaj funkcionalni nivo možete da postavite ukoliko imate kontrolere domena koje pokreću operativni sistemi Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2 ili Windows Server 2012. Funkcionalni nivo domena Windows Servera 2003 odlikuju sledeće osobine, koje postoje i na višim funkcionalnim nivoima domena:

- Zapisi atributa LastLogonTimestamp o tome kada se korisnik poslednji put prijavio na domen.
- *Ograničeno delegiranje* koje aplikacijama omogućava da bezbedno delegiraju ovlašćenja korisnika.

- *Selektivna provera autentičnosti* koja omogućava da konfigurišete određene resurse u šumi domena tako da se proverava autentičnost samo tačno određenim korisnicima ili grupama. Podrazumevano je postavljeno tako da je svim korisnicima u šumi domena dozvoljena provera autentičnosti pre provere ovlašćenja za te resurse.
- Podrška za čuvanje DNS zona u zasebnim oblastima što omogućava da selektivno vršite replikaciju DNS zona na određene kontrolere domena obuhvaćene tim zasebnim oblastima, umesto da konfigurišete replikaciju na sve kontrolere domena u domenu ili šumi.
- Replikacija na nivou atributa za grupe i druge atribute sa više vrednosti. Umesto replikacije čitavog objekta aktivnog direktorijuma, samo će promenjeni atributi biti replicirani.

### Funkcionalni nivo Windows Servera 2008

Funkcionalni nivo domena Windows Servera 2008 zahteva da se svi kontroleri domena izvršavaju na operativnim sistemima Windows Server 2008, Windows Server 2008 R2 ili Windows Server 2012. Pored svih osobina koje odlikuju funkcionalni nivo Windows Servera 2003, funkcionalni nivo domena Windows Servera 2008 obuhvata i sledeće:

- Poboljšanja u sistemu DFS (Distributed File System) replikacije koja omogućavaju da se replikacija obavlja mnogo efikasnije.
- Podršku za fino podešavanje pravila za raspodelu lozinki, što omogućava da primenite više zasebnih pravila za dodelu lozinki unutar istog domena.
- Podršku za lične virtuelne radne površine (Personal Virtual Desktops) korišćenjem altaki RemoteApp i Remote Desktop kada se koristi softver za virtuelizaciju Hyper-V.
- Kerberos podršku za AES 128 i 256 (AES: Advanced Encryption Services – napredni servisi šifrovanja).

### Funkcionalni nivo Windows Servera 2008 R2

Funkcionalni nivo domena Windows Servera 2008 R2 zahteva da se svi kontroleri domena izvršavaju na operativnim sistemima Windows Server 2008 R2 ili Windows Server 2012. Pored svih osobina koje odlikuju funkcionalne nivoe Windows Servera 2003 i Windows Servera 2008, ovaj funkcionalni nivo obuhvata i sledeće:

- Podršku za upravljanje nalozima servisa, koja omogućava da automatski upravljate lozinkama naloga servisa umesto da njima ručno upravljate.
- Podršku iz komandne linije za korpu za otpatke aktivnog direktorijuma ukoliko je funkcionalni nivo podignut na Windows Server 2008 R2.

### Funkcionalni nivo Windows Servera 2012

Funkcionalni nivo domena Windows Servera 2012 zahteva da se svi kontroleri domena izvršavaju na operativnom sistemu Windows Server 2012. Pored svih osobina koje odlikuju niže funkcionalne nivoe, ovaj funkcionalni nivo obuhvata i sledeće:

- Grupno upravljanje nalozima servisa, što omogućava da instalirate jedan nalog servisa na više računara.

- Podršku za fino podešavanje pravila za raspodelu lozinki putem alatke Active Directory Administrative Center, umesto da ih menjate alatkom ADSI Edit.
- Upravljanje korpom za otpatke aktivnog direktorijuma alatkom Active Directory Administrative Center umesto iz komandne linije ukoliko je šuma domena konfigurisana na funkcionalni nivo šume domena Windows Servera 2012.
- Ako je podrška za pristupanje, složenu proveru autentičnosti i Kerberos zaštitu u alatki za raspodelu šifara KDC (Key Distribution Center) postavljena tako da uvek podržava pristupanje (Always Provide Claims) ili odbija nezaštićene zahteve za proveru autentičnosti (Fail Unarmored Authentication Requests), ove opcije nisu dostupne ukoliko se funkcionalni nivo domena ne podigne na funkcionalni nivo Windows Servera 2012.

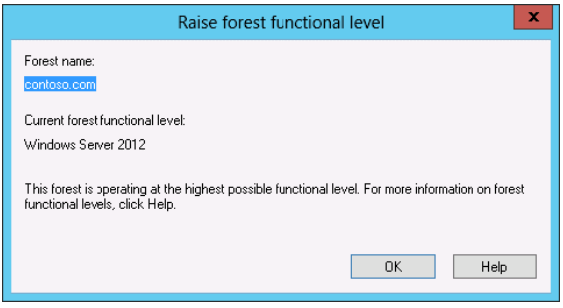
## Funkcionalni nivoi šume

Šuma može da obuhvata domene koji rade na različitim funkcionalnim nivoima domena. *Funkcionalni nivo šume* zavisi od najnižeg funkcionalnog nivoa domena bilo kog domena iz šume. Na primer, ukoliko vaša organizacija ima jedan domen koji se izvršava na funkcionalnom nivou Windows Servera 2008, a svi ostali domeni se izvršavaju na funkcionalnom nivou Windows Servera 2012, ne možete da podignete funkcionalni nivo šume na nivo viši od nivoa Windows Servera 2008. Funkcionalni nivo te šume možete da podignete na nivo Windows Servera 2012 tek pošto nivo tog jednog domena podignete sa funkcionalnog nivoa Windows Servera 2008 na funkcionalni nivo domena Windows Servera 2012.

***VIŠE INFORMACIJA*** **FUNKCIONALNI NIVOI**

Da biste o funkcionalnim nivoima naučili nešto više, pogledajte sledeći link: *http://technet.microsoft.com/enus/library/understanding-active-directory-functional-levels(v=ws.10).aspx*.

Funkcionalni nivo šume možete da podignete korišćenjem konzole Active Directory Domains and Trusts, kao što je prikazano na slici 1-3, ili korišćenjem komande Set-ADDomainMode Windows u komandnom prozoru PowerShell. Da biste to obavili, potrebno je da koristite nalog koji je član grupe Enterprise Admins. U opštem slučaju, ne možete da spustite funkcionalni nivo šume pošto ste ga podigli. Izuzetak od ovog pravila je da možete spustiti funkcionalni nivo šume sa nivoa Windows Servera 2012 na nivo Windows Servera 2008 R2 ukoliko pre toga niste omogućili korišćenje korpe za otpatke aktivnog direktorijuma.




**SLIKA 1-3** Podizanje funkcionalnog nivoa šume

Mada je korišćenje korpe za otpatke aktivnog direktorijuma dostupno na funkcionalnom nivou šume Windows Servera 2008 R2, potrebno je da konfigurišete šumu u vašoj organizaciji tako da se izvršava na funkcionalnom nivou šume Windows Servera 2012 kako biste mogli da koristite alatku Active Directory Administrative Center umesto prozora sa komandnom linijom. Postavljanje funkcionalnog nivoa šume Windows Servera 2012 ne uvodi druge mogućnosti, već se time šuma ograničava na to da koristi samo kontrolere domena koji se izvršavaju na Windows Server 2012 ili novijoj verziji operativnog sistema Windows Server.

**Brza provera**

- Koji je najniži funkcionalni nivo šume koji vam omogućava da primenjujete korpu za otpatke aktivnog direktorijuma?

**Odgovor**

- Korpu za otpatke aktivnog direktorijuma možete da primenjujete na funkcionalnom nivou šume Windows Servera 2008 R2.

## Okruženje aktivnog direktorijuma sa više šuma

Ne samo da mnoge organizacije imaju više od jednog domena u svojim šumama, već neke organizacije imaju više šuma aktivnog direktorijuma. Veći broj šuma obično nastaje kada jedna organizacija preuzima drugu organizaciju, tokom perioda pre nego što organizacija koja vrši preuzimanje ne preuzme za sebe infrastrukturu preuzete organizacije.

Ostali razlozi zbog koji imamo više šuma aktivnog direktorijuma unutar jedne organizacije obuhvataju:

- **Bezbednosne zahteve** Administratori iz jednog dela organizacije neće imati prava u drugom delu organizacije time što će se svaki deo organizacije nalaziti u zasebnim šumama.
- **Neuskladive šeme** Svi domeni u šumi dele šemu. Ukoliko su za dva različita dela u organizaciji potrebne dve zasebne šeme, nepohodna je primena više šuma.
- **Političke zahteve** Multinacionalne organizacije ponekad moraju da poštuju drugačije pravne zahteve. Da bi se takvi zahtevi ispunili, ponekad je jednostavnije napraviti zasebne šume sa odnosima poverenja, nego da se domeni unutar iste šume konfigurišu tako kako bi se usaglasili svi zahtevi.

## Nadogradnja postojećih domena i šuma

Možete koristiti jednu od dve moguće strategije prilikom nadogradnje postojećeg domena kako biste ga konfigurisali na funkcionalni nivo Windows Servera 2012:

- Prva strategija je da na svakom kontroleru domena nadogradite operativne sistema na Windows Server 2012. Ovaj metod može da bude problematičan, pošto mnoge organizacije koriste Windows Server 2003 na kontrolerima domena, a Windows Server 2003 ne možete direktno da nadogradite na Windows Server 2012. Takođe, vrlo je verovatno da se postojeći kontroleri domena izvršavaju na x86 verziji Windows Server operativnog sistema. Windows operativni sistemi nikada ne podržavaju direktnu nadogradnju sa x86 verzija na x64 verzije.
- Možete da uvedete Windows Server 2012 kontrolere domena u postojeći domen, a da zatim povučete iz upotrebe postojeće kontrolere domena koji se izvršavaju na starijim verzijama Windows Server operativnog sistema. Ovaj metod je manje složen od izvođenja direktne nadogradnje. Ukoliko hardver to podržava, možete promeniti svrhu postojećem hardveru tako da kontroleri domena povučeni iz upotrebe imaju novu namenu kao Windows Server 2012 kontroleri domena (mada sve veći broj organizacija ima kontrolere domena koji se izvršavaju na virtuelnim računarima).

Za razliku od ranijih načina za nadogradnju kontrolera domena, ne morate direktno da pokrećete komandu adprep.exe kako biste pripremili aktivni direktorijum za uvođenje kontrolera domena koji se izvršavaju na Windows Serveru 2012. Umesto toga, ukoliko prilikom uvođenja prvog Windows Server 2012 kontrolera domena koristite nalog koji je član Schema Admins and Enterprise Admins grupe, nadogradnja šeme se dešava automatski. Potrebno je da pokrenete komandu adprep.exe samo u slučaju da obavljate nadogradnju postojećih kontrolera domena koji se izvršavaju na x64 verziji Windows Servera 2008 ili Windows Servera 2008 R2 i ukoliko će taj nadograđeni kontroler domena biti prvi Windows Server 2012 kontroler domena u tom domenu.

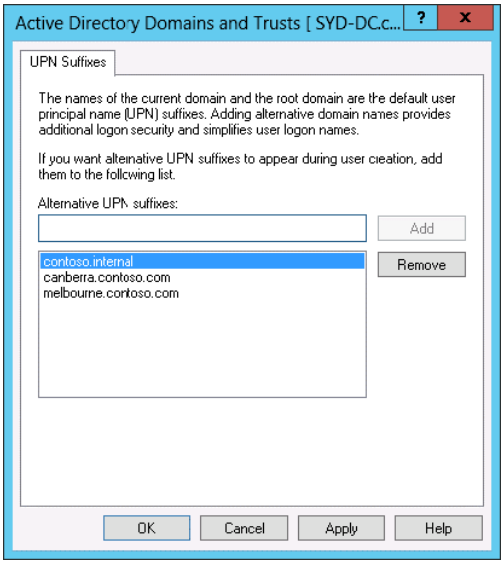
***NAPOMENA*** **ALATKA ACTIVE DIRECTORY MIGRATION**

Alatka Active Directory Migration može da vam pomogne pre u slučaju premeštanja postojećeg okruženja aktivnog direktorijuma nego u slučaju nadogradnje postojećeg okruženja. Verzija 3.2 alatke Active Directory Migration nije podržana na Windows Serveru 2012.

## Sufiksi osnovnog korisničkog imena (UPN – User Principal Name)

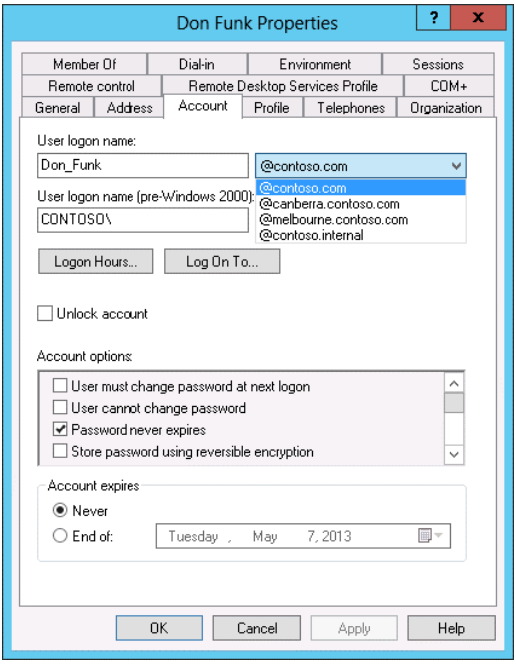
Sufiksi osnovnog korisničkog imena (UPN sufiksi) deo su osnovnog korisničkog imena koji sledi iza simbola @. Na primer, u osnovnom korisničkom imenu don_funk@contoso.com, UPN sufiks je ime domena contoso.com. UPN sufiksi omogućavaju korisnicima da se prijave koristeći ime naloga koje obuhvata ime njihovih domena. Pošto UPN sufiksi liče na elektronske adrese, korisnici ih lako pamte. To je korisno u složenim okruženjima u kojima korisnici mogu da se prijave na računare koji su članovi domena koji se razlikuju od domena na kome su smešteni njihovi nalozi. Na primer, korisnički nalog Kim Aker može da se nalazi na domenu accounts.contoso.com, a njoj je potrebno da se prijavi na računar koji je član domena computers.contoso.com. Umesto da se prijavi koristeći accounts\kim_akers kao svoje korisničko ime, ili da bira domen accounts sa spiska, što bi inače morala da uradi, ona se jednostavno prijavljuje koristeći UPN u obliku kim_akers@contoso.com.

Podrazumevano svi korisnici koriste UPN sufiks koji je ime korenog domena i pored toga što se njihovi nalozi nalaze u domenu potomku. Na taj način Kim može da se prijavi kao kim_akers@contoso.com pošto je contoso.com UPN sufiks korenog domena. UPN sufikse konfigurišete korišćenjem konzole Active Directory Domains and Trusts kao što je prikazano na slici 1-4.




**SLIKA 1-4** Konfugurisanje alternativnih UPN sufiksa

UPN sufikse pridružene određenom korisničkom nalogu možete da konfigurišete na kartici Account u okviru sa osobinama naloga putem konzole Active Directory Users and Computers kao što je prikazano na slici 1-5. Prilikom konfigurisanja poverenja unutar šume možete da sprečite ili dozvolite proveru autentičnosti korisnika na osnovu UPN sufiksa.




**SLIKA 1-5** Konfigurisanje određenog UPN sufiksa

***VIŠE INFORMACIJA*** **UPN SUFIKSI**

Da biste o UPN sufiksima naučili nešto više, pogledajte sledeći link: *http://technet.microsoft.com/enus/library/cc772007.aspx*.

## Pregled lekcije

- Šuma može da sadrži više domena. Domeni stabla grade se na istom prostoru imena. Šuma može da sadrži veći broj domena stabla.
- Nijedno ime matičnog računara u šumi aktivnog direktorijuma ne može da bude duže od 64 znaka.
- Funkcionalni nivo domena zavisi od najstarije verzije operativnog sistema Windows Server koja se koristi na nekom kontroleru domena u tom domenu.
- Funkcionalni nivo domena određuje koja se najniža verzija operativnog sistema Windows Server može koristiti na kontrolerima domena.
- Svaki domen u šumi može da ima drugačiji funkcionalni nivo. Funkcionalni nivo šume zavisi od najnižeg funkcionalnog nivoa domena u šumi.
- Možete da koristite prilagođene UPN sufikse kako biste pojednostavili proces prijavljivanja za korisnike u okruženjima sa više domena i šumama sa više domena.

## Obnavljanje lekcije

Odgovorite na sledeća pitanja kako biste proverili svoje znanje o informacijama iz ove lekcije. Odgovore na ova pitanja i objašnjenja o svakom odgovoru možete pronaći u odeljku „Odgovori" na kraju ovog poglavlja.

1. U postupku ste planiranja primene novog aktivnog direktorijuma za svoju organizaciju. Dva različita odseka u vašoj organizaciji će primenjivati aplikacije koje imaju zasebne i međusobno isključive zahteve za šemu aktivnog direktorijuma. Koju od sledećih struktura aktivnog direktorijuma bi trebalo da koristite kako biste ispunili ove zahteve?

   **A.** Jednu šumu sa jednim domenom stablom

   **B.** Jednu šumu sa više domena stabla

   **C.** Više šuma

   **D.** Šumu sa jednim domenom

2. Radite kao sistem administrator za kompaniju Tailspin Toys i njenu podružnicu Wingtip Toys. U postupku ste planiranja strukture za novi aktivni direktorijum. Od vas se traži da obezbedite to da se zaposleni koji rade u delu organizacije Tailspin Toys prijavljuju na domen koji se zove tailspintoys.com, a da se zaposleni koji rade u delu organizacije Wingtip Toys prijavljuju na domen koji se zove wingtiptoys.com. Želite to da uradite na najjedostavniji mogući način i da smanjite stvaranje odnosa poverenja. Koju od sledećih struktura aktivnog direktorijuma bi trebalo da koristite kako biste ispunili ove zahteve?

   **A.** Šumu sa jednim domenom

   **B.** Više šuma

   **C.** Jednu šumu sa više domena stabla

   **D.** Jednu šumu sa jednim domenom stablom

3. Želite da postavite nekoliko kontrolera domena koji se izvršavaju na operativnom sistemu Windows Server 2012. Na kraju ćete postojeće kontrolere domena povući iz upotrebe i domen podići na funkcionalni nivo domena Windows Servera 2012. Koji najniži funkcionalni nivo domena je potreban da bi se podržalo uvođenje kontrolera domena koji se izvršavaju na operativnom sistemu Windows Server 2012?

   **A.** Funkcionalni nivo domena Windows Servera 2003

   **B.** Funkcionalni nivo domena Windows Servera 2008

   **C.** Funkcionalni nivo domena Windows Servera 2008 R2

   **D.** Funkcionalni nivo domena Windows Servera 2012

4. Na kojim funkcionalnim nivoima šume je dostupna korpa za otpatke aktivnog direktorijuma? (Izaberite sve moguće tačne odgovore.)

**A.** Na funkcionalnom nivou šume Windows Servera 2012

**B.** Na funkcionalnom nivou šume Windows Servera 2008 R2

**C.** Na funkcionalnom nivou šume Windows Servera 2008

**D.** Na funkcionalnom nivou šume Windows Servera 2003

# Lekcija 2: Konfigurisanje poverenja

S vremena na vreme neophodno je povezati dva različita domena kako bi korisnici koji imaju naloge u jednom domenu mogli da pristupaju resursima u drugom domenu. Ukoliko ti domeni pripadaju istoj organizaciji, najjednostavniji način da se to uradi je konfigurisanjem poverenja. U ovoj lekciji saznaćete kako da konfigurišete poverenje između dve različite šume, između dva zasebna domena u različitim šumama i između domena i Kerberos oblasti.

**Posle ove lekcije moći ćete da:**

- konfigurišete eksterna poverenja, poverenja između šuma, preča poverenja i poverenja između oblasti
- konfigurišete proveru autentičnosti poverenja
- konfigurišete SID filtriranje
- konfigurišete rutiranje sufiksa imena

**Očekivano trajanje lekcije: 45 minuta**

## Poverenja

Poverenja (engl. *trusts*) omogućavaju da identifikaciju korisnika iz jednog domena vrše kontroleri domena iz zasebnog domena. Na primer, ukoliko postoji dvosmerni odnos poverenja između domena contoso.local i adatum.remote, korisnici sa nalozima u domenu contoso.local mogu da se identifikuju u domenu adatum.remote. Konfigurisanjem odnosa poverenja, moguće je dopustiti korisnicima iz jednog domena da pristupaju resursima u drugom domenu, tako da mogu da koriste deljene foldere i štampače ili da se prijavljuju za rad na računarima koji su članovi drugih domena u odnosu na računare na kojima se nalaze njihovi korisnički nalozi.

Neka poverenja nastaju automatski. Na primer, domeni u istoj šumi automatski imaju međusobno poverenje. Druga poverenja, kao što su eksterna poverenja, poverenja između oblasti, preča poverenja i poverenja između šuma moraju se napraviti ručno. Poverenja podrazumevano koriste Kerberos V5 protokol za proveru autentičnosti, ali mogu da se vrate na korišćenje NTLM protokola ukoliko Kerberos V5 nije podržan. Poverenja konfigurišete i njima upravljate korišćenjem konzole Active Directory Domains and Trusts ili alatkom netdom.exe iz komandne linije sa opcijom trust.

***U PRAKSI*** **RAZUMEVANJE POVERENJA**

Mada sama reč poverenje ne stvara mnogo zabuna oko svog značenja, terminologija koja se koristu u vezi sa poverenjem može da zbuni većinu ljudi. Veoma je važno da razumete razliku između domena koji daje poverenje i domena koji prima poverenje i kako smer davanja poverenja, dolazni i odlazni, ima veze sa tim za koje bezbedne učesnike će moći da se vrši provera autentičnosti.

Da biste razumeli poverenja, potrebno je da razumete razliku između domena ili šume koji daju poverenje i domena ili šume koji primaju poverenje. Domen ili šuma koji daju poverenje obuhvataju resurse za koja želite da dodelite bezbednosna ovlašćenja za pristup sa domena ili šume koji primaju poverenje. Domen ili šuma koji primaju poverenje drže bezbedne učesnike kojima želite da dozvolite pristup resursima u šumi koja daje poverenje. Na primer, ukoliko želite da korisnicima u domenu adatum.remote dopustite pristup resursima u domenu contoso.local, domen adatum.remote je domen koji daje poverenje, a domen contoso.local je domen koji prima poverenje. U dvosmernom odnosu poverenja, domen ili šuma su istovremeno i davaoci i primaoci poverenja.

***VIŠE INFORMACIJA*** **POVERENJA**

Da biste o osnovama poverenja naučili nešto više, pogledajte sledeći link:
*http://technet.microsoft.com/en-us/library/cc731335.aspx*.

## Tranzitivnost poverenja

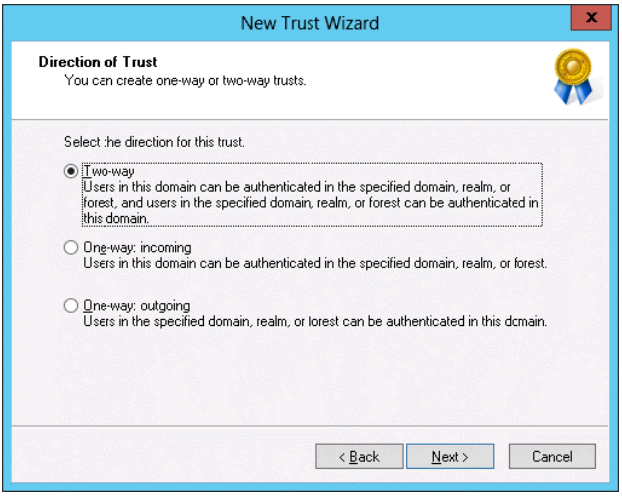
*Tranzitivno poverenje* je ono koje se širi izvan granica prvobitnog domena poverioca. Na primer, ukoliko imate poverenje između dve šume domena i to poverenje je tranzitivno, svi domeni u obe šume imaće međusobno poverenje. Poverenje između šuma je podrazumevano tranzitivno. Eksterna poverenja podrazumevano nisu tranzitivna. Kada pravite poverenje, vodite računa o tome da možda postoje domeni iza onoga sa kojim uspostavljate odnos, a koji time mogu biti obuhvaćeni. Možda verujete administratoru domena adatum.remote da neće dozvoliti pristup nedobronamernim korisnicima, ali da li verujete administratoru njegovog podomena subdomain. adatum.remote?

***VIŠE INFORMACIJA*** **TRANZITIVNOST POVERENJA**

Da biste o tranzitivnosti poverenja naučili nešto više, pogledajte sledeći link:
*http://technet.microsoft.com/en-us/library/cc754612.aspx*.

## Smer poverenja

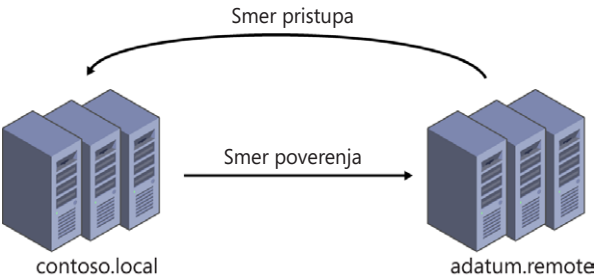
Kada pravite novo poverenje, smer poverenja određujete kao što je prikazano na slici 1-6. Možete da izaberete poverenje u oba smera (onosno, dvosmerno poverenje) ili jednosmerno poverenje, koje može da bude ili u jednom smeru dolazno ili u jednom smeru odlazno.




**SLIKA 1-6** Određivanje smera poverenja

Kada konfigurišete jednosmerno dolazno poverenje, autentičnost korisnika u lokalu se proverava u udaljenom domenu, oblasti ili šumi. Upamtite to da ukoliko konfigurišete jednosmerno dolazno poverenje između šuma sa jednim domenom contoso.local i adatum.remote, korisnici sa nalozima u domenu contoso.local mogu da pristupaju resursima u domenu adatum.remote. Slično tome, ukoliko konfigurišete jednosmerno odlazno poverenje između šuma sa jednim domenom contoso.local i adatum.remote, korisnici sa nalozima u domenu adatum.remote mogu da pristupaju resursima koji se nalaze u domenu contoso.local.

Terminologija koja se koristi za poverenja može da bude pomalo zbunjujuća. Ključna stvar koju treba upamtiti je da je smer poverenja suprotan smeru pristupa, kao što je prikazano na slici 1-7. Odlazno poverenje dozvoljava dolazni pristup, a dolazno poverenje dozvoljava odlazni pristup.




**SLIKA 1-7** Smer poverenja i smer pristupa

***VIŠE INFORMACIJA*** **SMER POVERENJA**

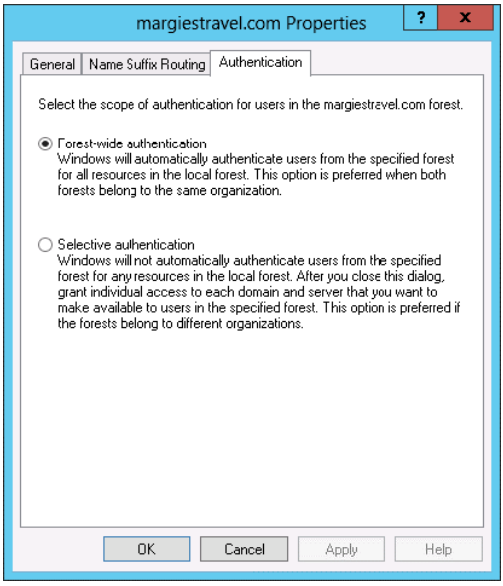
Da biste o smerovima poverenja naučili nešto više, pogledajte sledeći link: *http://technet.microsoft.com/en-us/library/cc731404.aspx.*

## Poverenje između šuma

Kada konfigurišete poverenje između šuma, jedna šuma aktivnog direktorijuma daje poverenje drugoj šumi. Poverenja između šuma su tranzitivna. Kada konfigurišete poverenje između šuma, bilo kom domenu u šumi koja daje poverenje dozvoljavate da bude dostupan svim bezbednim učesnicima iz šume koja prima poverenje. Poverenja između šuma zahtevaju da sve šume budu konfigurisane tako da se izvršavaju na funkcionalnom nivou šume Windows Servera 2003 ili višem. Poverenja između šuma mogu da budu dvosmerna ili jednosmerna. Poverenja između šuma ćete najverovatnije konfigurisati ukoliko vaša organizacija ima aktivan direktorijum sa dve šume ili sa više njih.

Možete da konfigurišete jedan od dva načina za proveru autentičnosti kada konfigurišete poverenje između šuma. Koji ćete način za proveru autentičnosti koristiti zavisi od vaših bezbednosnih zahteva. Opcije su:

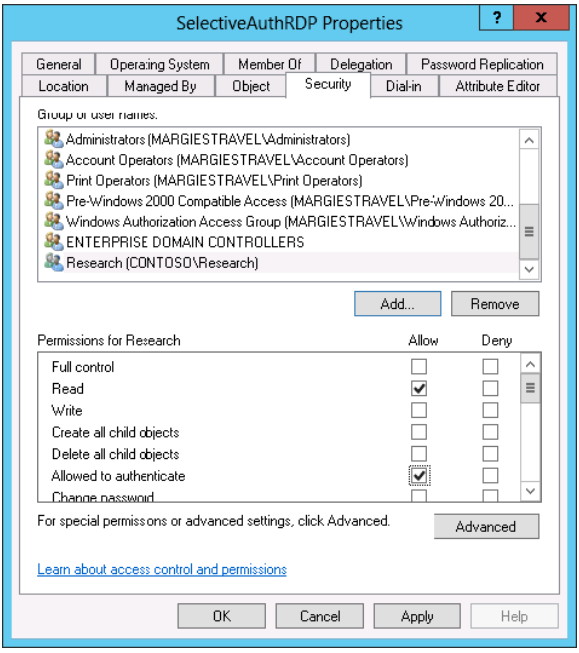
- **Provera autentičnosti za čitavu šumu** Kada izaberete proveru za čitavu šumu, provera autentičnosti za sve korisnike iz šume koja prima poverenje automatski se vrši za sve resurse u toj šumi. Ovu opciju bi trebalo da izaberete kada su i šuma koja daje i šuma koja prima poverenje deo iste organizacije. Na slici 1-8 prikazano je poverenje između šuma konfigurisano ovim tipom provere autentičnosti.
- **Selektivna provera autentičnosti** Kada konfigurišete ovu opciju, Windows ne vrši automatsko proveravanje autentičnosti korisnika iz šume koja prima poverenje. U tom slučaju možete da konfigurišete određene servere i domene unutar šume tako da vrše proveru autentičnosti korisnika iz šume koja prima poverenje. Ovu opciju koristite kada dve šume pripadaju različitim organizacijama ili ukoliko imate znatno strožije bezbednosne zahteve.




**SLIKA 1-8** Konfigurisanje načina za proveru autentičnosti

## Konfigurisanje selektivne provere autentičnosti

Konfigurisanje slelektivne provere autentičnosti znači da se tačno određenim bezbednim učesnicima iz šume koja prima poverenje dozvoljava provera autentičnosti (opcija Allowed to authenticate (allow)) na računaru na kome se nalaze resursi kojima želite da dopustite pristup. Na primer, pretpostavimo da ste konfigurisali poverenje između šuma sa selektivnom proverom autentičnosti. Želite da korisnicima u opštoj grupi Research iz šume koja prima poverenje dozvolite pristup serveru Remote Desktop Services (RDS) u šumi koja daje poverenje. Da biste ostavarili ovaj cilj, konzolom Active Directory Users and Computers konfigurišete osobine računarskog naloga RDS servera i dozvoljavate da se vrši provera autentičnosti (opcija Allowed to authenticate) za opštu grupu Research iz šume koja prima poverenje, kao što je prikazano na slici 1-9. Na taj način vrši se provera autentičnosti samo za korisnike iz te grupe; a još uvek možete da im dozvolite pristup do RDS servera tako što ćete ih dodati u odgovarajuću grupu na samom RDS serveru.




**SLIKA 1-9** Konfigurisanje opcije Allowed to authenticate (dozvoljena provera autentičnosti)

## Eksterna poverenja

Eksterna poverenja omogućavaju da konfigurišete jedan domen u jednoj šumi tako da ima poverenje u domen u drugoj šumi bez korišćenja tranzitivnog poverenja. Na primer, konfigurišete eksterno poverenje ukoliko želite da dozvolite da domen auckland.fabrikam.com uspostavi odnos poveranja sa domenom wellington.adatum.com, a da svi ostali domeni u šumama fabrikam.com ili adatum.com pri tome ne uspostave međusobne odnose poverenja.

***VIŠE INFORMACIJA*** **EKSTERNA POVERENJA**

Da biste o eksternim poverenjima naučili nešto više, pogledajte sledeći link: *http://technet.microsoft.com/en-us/library/cc732859.aspx*.

Eksterno poverenje koristite da biste konfigurisali odnose poverenja sa domenima koji se izvršavaju na nepodržanim Windows Server operativnim sistemima, kao što su Windows 2000 Server i Windows NT 4.0, pošto ti sistemi ne podržavaju poverenje između šuma. Bez obzira na to što su ti operativni sistemi davno zastareli, još uvek ima organizacija sa serverima i čak domenima koje pokreću ti operativni sistemi. Moguće je, mada je malo verovatno, da će biti potrebno da konfigurišete odnos poverenja između domena koji pokreću ti operativni sistemi i kontrolera domena koji se izvršava na Windows Serveru 2012.

**Brza provera**

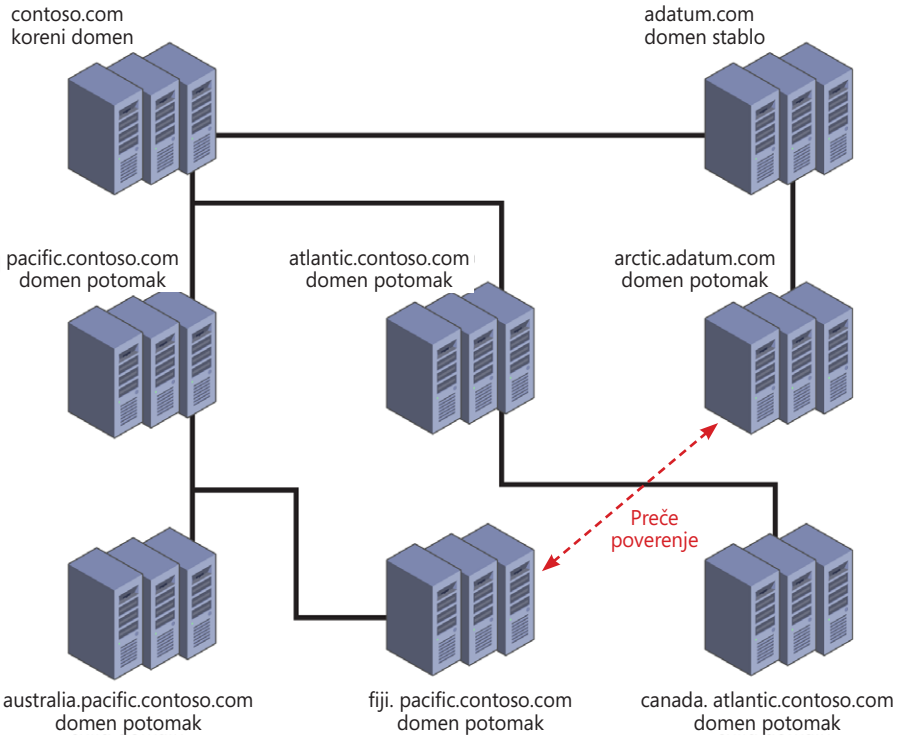
- Administrator ste šume sa jednim domenom contoso.local. Korisnicima u šumi sa jednim domenom adatum.remote neophodan je pristup resursima u domenu contoso.local. Korisnicima u domenu contoso.local ne treba pristup do resursa u domenu adatum.remote. Konfigurišete eksterno poverenje između te dve šume sa po jednim domenom iz domena contoso.local. Koji bi smer poveranja trebalo da konfigurišete da biste ostvarili ovakvu konfiguraciju?

**Odgovor**

- Jedosmerni odlazni. Sećate se da je smer poverenja suprotan smeru provere autentičnosti. Da biste proverili autentičnost korisnika u dolaznom smeru, konfigurišete poverenje sa odlaznim smerom.

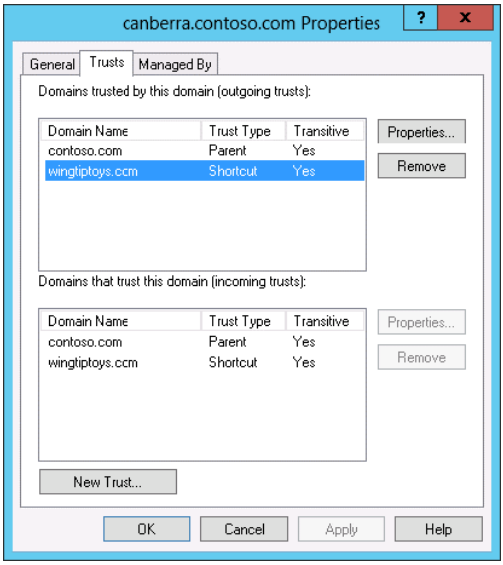
## Preče poverenje

*Preče poverenje* (engl. *shortcut trust*) omogućava da ubrzate proveru autentičnosti između domena u šumi koji se nalaze u zasebnim granama ili čak u zasebnim stablima. Na primer, u hipotetičkoj šumi prikazanoj na slici 1-10, ukoliko korisnik u domenu fiji.pacific.contoso.com želi da pristupi resursima u domenu arctic.adatum.com, bilo bi potrebno da provera autentičnosti putuje kroz domene pacific.contoso.com i contoso.com pre nego što prođe kroz domen adatum.com da bi konačno stigla do domena arctic.adatum.com. Ukoliko primenite preče poverenje između domena fiji.pacific.contoso.com i arctic.adatum.com, provera autentičnosti mogla bi da se vrši direktno između ta dva domena bez potrebe da se ta dva domena stabla u šumi poprečno povežu.




**SLIKA 1-10** Preče poverenje

Preče poverenje konfigurišete korišćenjem konzole Active Directory Domains and Trusts menjanjem osobina jednog domena i pokretanjem čarobnjaka New Trust Wizard na kartici Trusts. Kada se poverenje uspostavi, pojavljuje se kao Shorcut trust (preče poverenje) kao što je prikazano na slici 1-11. Preče poverenje može biti jednosmerno ili dvosmerno. Kao i u slučaju sa pravljenjem ostalih poverenja, proverite da li razrešavanje imena radi ispravno između domena koji daje poverenje i domena koji prima poverenje bilo tako što se zone sistema imenovanja domena (DNS – Domain Name System) prenose kroz šumu, tako što se konfigurišu uslovni prosleđivači ili tako što se konfigurišu prividne zone.




**SLIKA 1-11** Preče poverenje

## Poverenje između oblasti

Poverenje između oblasti koristite da biste napravili odnos između domena servisa aktivnog direktorijuma i Kerberos V5 oblasti koja koristi servis direktorijuma drugog proizvođača. Poverenje između oblasti može biti tranzitivno ili netranzitivno. Takođe, može da bude jednosmerno i dvosmerno. Najverovatniji slučaj za konfigurisanje poverenja između oblasti je onaj kada vam treba da korisnicima koji koriste UNIX servis direktorijuma dozvolite pristup do resursa u domenu aktivnog direktorijuma ili kada korisnici iz domena aktivnog direktorijuma treba da pristupe resursima u oblasti UNIX Kerberos V5.

Poverenje između oblasti konfigurišete korišćenjem konzole Active Directory Domains and Trusts. To radite na taj način što birate opciju Realm trust (poverenje između oblasti), kao što je prikazano na slici 1-12. Prilikom konfigurisanja poverenja između oblasti, određujete lozinku za poverenje između oblasti koju ćete koristiti prilikom konfigurisanja druge strane poverenja u Kerberos V5 oblasti.