

## Poglavlje 1

# Instalacija

Servisi domena aktivnog direktorijuma (Active Directory Domain Services – AD DS) i njegovi srodni servisi formiraju osnovu da računarska mreža preduzeća koja koristi operativni sistem Microsoft Windows zajedno deluje u vidu alatki za skladištenje informacija o identitetima korisnika, računara i servisa; da proveriti identitet korisnika ili računara i da obezbedi mehanizam kojim će korisnik ili računar moći da pristupi resursima u preduzeću. U ovom poglavlju počecete svoje istraživanje aktivnog direktorijuma Windows Servera 2008 tako što ćete instalirati ulogu servisa domena aktivnog direktorijuma i kreirati kontroler domena u novoj šumi aktivnog direktorijuma. Videćete da Windows Server 2008 nastavlja da razvija aktivni direktorijum poboljšavanjem brojnih koncepata i karakteristika sa kojima ste se upoznali kroz vaše iskustvo sa aktivnim direktorijumom.

Ovo poglavlje se fokusira na kreiranje nove šume aktivnog direktorijuma pomoću jednog domena na jednom kontroleru domena. Praktična vežbanja u ovom poglavlju sprovedeće vas kroz kreiranje domena koji se zove *contoso.com* i koji ćete koristiti za sve ostale vežbe u ovom udžbeniku za pripremu ispita. Kasnije, u poglavlju 8 „Provera identiteta”, poglavlju 10 „Kontroleri domena” i poglavlju 12 „Domeni i šume”, naučićete da implementirate druge situacije, uključujući šume sa više domena, nadogradnje postojećih šuma u Windows Server 2008 i napredne opcije instalacije. U poglavljima 14 „Servisi jednostavnog direktorijuma u aktivnom direktorijumu”, 15 „Servisi sertifikata aktivnog direktorijuma”, 16 „Servisi upravljanja pravima aktivnog direktorijuma” i 17 „Servisi ujedinjenja aktivnog direktorijuma”, saznaćete detalje o drugim servisima aktivnog direktorijuma kao što su servisi jednostavnog direktorijuma u aktivnom direktorijumu (Active Directory Lightweight Directory Services), servisi sertifikata aktivnog direktorijuma (Active Directory Certificate Services) i infrastruktura javnih ključeva, servisi upravljanja pravima aktivnog direktorijuma (Active Directory Rights Management Services) i servisi ujedinjenja aktivnog direktorijuma (Active Directory Federation Services).

### Ciljevi ispita u ovom poglavlju su:

- Konfigurisanje infrastrukture aktivnog direktorijuma;
  - Konfigurirate šumu ili domen.

### Lekcije u ovom poglavlju su:

- Lekcija 1: Instaliranje servisa domena aktivnog direktorijuma . . . . .3
- Lekcija 2: Servisi domena aktivnog direktorijuma na jezgru servera . . . . .23

## Pre nego što počnete

Kako biste obradili lekcije u ovom poglavlju, treba da uradite sledeće:

- Nabavite dva računara na kojima ćete instalirati Windows Server 2008. Računari mogu biti fizički sistemi koji ispunjavaju minimalne uslove za Windows Server 2008, koje možete naći na <http://technet.microsoft.com/en-us/windowsserver/2008/bb414778.aspx>. Trebaće vam najmanje 512 MB RAM-a, 10 GB slobodnog mesta na hard disku i x86 procesor sa minimalnim radnim taktom od 1 GHz ili x64 procesor sa minimalnim radnim taktom od 1,4 GHz. Kao alternativu možete koristiti virtuelne mašine koje ispunjavaju iste uslove.
- Nabavite probnu verziju Windows Servera 2008. U trenutku pisanja ove knjige, veze ka probnim verzijama dostupne su na Windows Server 2008 početnoj internet strani <http://www.microsoft.com/windowsserver2008>.

### U praksi

*Dan Holme*

Kontroleri domena izvode funkcije upravljanja identitetom i pristupom koje su kritične za integritet i bezbednost Windows sistema poslovanja. Zbog toga većina organizacija bira da posveti ulogu kontrolera domena, što znači da kontroler domena ne pruža druge funkcije kao što su serveri datoteka i štampača. Međutim, kada je u prethodnim verzijama Windowsa server unapređen u kontroler domena, ostali servisi su i dalje bili dostupni, bez obzira na to da li su u upotrebi ili ne. Ovi dodatni nepotrebni servisi povećavaju potrebu za primenjivanjem zakrpa i ažuriranja bezbednosti i izlaganjem kontrolera domena dodatnoj podložnosti za napad. Windows Server 2008 pristupa ovim razmatranjima kroz svoju arhitekturu, koja se zasniva na ulozi tako što server započinje svoj život poput prilično jednostavne instalacije Windowsa kojoj se dodaju uloge i njihovi udruženi servisi i karakteristike. Osim toga, nova instalacija jezgra servera (Server Core) Windows Servera 2008 pruža minimalnu instalaciju Windowsa koja čak napušta grafičko korisničko okruženje (GUI) u korist komandnog odzivnika. U ovom poglavlju steći ćete neposredno iskustvo sa ovim značajnim karakteristikama kontrolera domena Windows Servera 2008. Ove promene u arhitekturi i skupu karakteristika Windows Servera 2008 pomoći će vama i drugim preduzećima da još više unapredite bezbednost, stabilnost i podesivost vašeg upravljanja infrastrukturom identiteta i pristupa.

## Lekcija 1: Instaliranje servisa domena aktivnog direktorijuma

Servisi domena aktivnog direktorijuma (AD DS) pružaju funkcionalnost rešenja identiteta i pristupa (IDA) za računarske mreže preduzeća. U ovoj lekciji učićete o AD DS-u i drugim ulogama aktivnog direktorijuma koje podržava Windows Server 2008. Takođe ćete istražiti Server Manager, alatku kojom možete konfigurisati uloge servera i unapređenog čarobnjaka Directory Domain Services Installation. Ova lekcija se takođe osvrće i na ključne koncepte IDA-e i aktivnog direktorijuma.

Po završetku ove lekcije, moći ćete da:

- Objasnite ulogu identiteta i pristupa u računarskoj mreži preduzeća.
- Razumete odnos između servisa aktivnog direktorijuma.
- Konfigurirate kontroler domena pomoću uloge servisa domena aktivnog direktorijuma (AD DS) koristeći Windows okruženje.

Procenjeno vreme za lekciju: 60 minuta

### Aktivni direktorijum, identitet i pristup

Kao što je pomenuto u uvodnom delu poglavlja i ove lekcije, aktivni direktorijum pruža IDA rešenje za računarske mreže preduzeća koje koriste Windows. IDA su neophodni kako bi se održavala bezbednost resursa preduzeća kao što su datoteke, elektronska pošta, aplikacije i baze podataka. IDA infrastruktura bi trebalo da obavlja sledeće:

- **Skladišti informacije o korisnicima, grupama, računarima i drugim identitetima** Identitet je, u širem smislu reči, prikaz entiteta koji će izvoditi operacije u računarskoj mreži preduzeća. Na primer, neki korisnik će otvoriti dokumente iz zajedničke fascikle na serveru. Dokument će biti obezbeđen ovlašćenjima na listi za kontrolu pristupa (ACL). Za pristup dokumentu upravlja se podsistemom bezbednosti servera, koji poređi identitet korisnika sa identitetima na ACL-u kako bi se ustanovilo da li će pristup korisnika biti odobren ili odbijen. Računari, grupe, servisi i drugi objekti takođe izvode operacije na mreži i moraju biti predstavljeni identitetima. Među usklađenim informacijama o identitetu nalaze se svojstva koja jedinstveno identifikuju objekat, kao što su korisničko ime ili bezbednosni identifikator (SID) i lozinka za identitet. *Skladište identiteta (Identity Store)* je, prema tome, jedna komponenta IDA infrastrukture. Skladište podataka aktivnog direktorijuma, poznato i kao direktorijum, predstavlja skladište identiteta. Sam direktorijum se čuva na kontroleru domena – serveru koji obavlja AD DS ulogu, koji takođe i upravlja ovim direktorijumom.

- **Proveri identitet** Server korisniku neće odobriti pristup dokumentu sve dok ne verifikuje da je identitet koji je predstavljen u zahtevu za pristup validan. Kako bi potvrdio identitet, korisnik otkriva tajne koje znaju samo on i IDA infrastruktura. Te tajne se porede sa informacijom u skladištu identiteta, u procesu koji se naziva *provera identiteta* (*Authetication*).

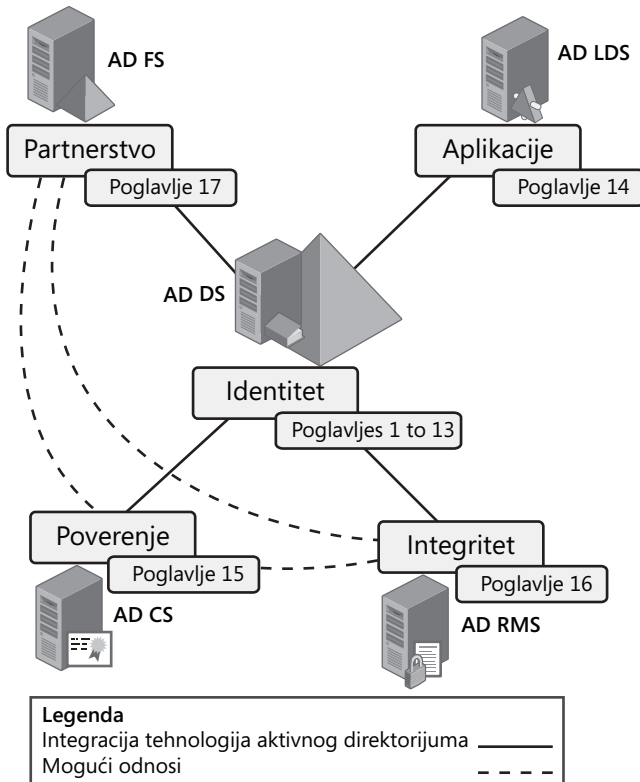
### **Kerber provera identiteta u domenu aktivnog direktorijuma**

U domenu aktivnog direktorijuma, za proveru identiteta koristi se protokol pod nazivom Kerber (Kerberos). Kada se korisnik ili računar prijavi na domen, Kerber proverava njegove identifikatore i izdaje paket informacija koji se naziva karta za dodelu karata (Ticket Granting Ticket – TGT). Pre nego što se korisnik poveže sa serverom kako bi zatražio neki dokument, Kerber zahtev se šalje kontroleru domena zajedno sa TGT-om, koji identifikuje proverenog korisnika. Kontroler domena izdaje korisniku još jedan paket informacija koji se naziva servisna karta (Service Ticket), koja serveru identifikuje proverenog korisnika. Korisnik podnosi servisnu kartu serveru, koji je prihvata kao dokaz da je identitet korisnika proveren.

Ove Kerber transakcije za rezultat imaju jedinstvene prijave na mrežu. Nakon što se korisnik ili računar inicijalno prijavio i nakon što mu je dodeljen TGT, proverava se identitet korisnika unutar celog domena i mogu mu se dodeliti servisne karte koje identifikuju korisnika bilo kom servisu. Celokupnim procesom izdavanja karata upravljaju Kerber klijenti i servisi koji su ugrađeni u Windows, i on je korisniku transparentan.

- **Kontroliše pristup** IDA infrastruktura je odgovorna za zaštitu poverljivih informacija, kao što su informacije koje su smeštene u dokumentu. Pristupom poverljivom dokumentu mora se upravljati u skladu sa pravilima preduzeća. ACL na dokumentu predstavlja politiku bezbednosti koja je sačinjena od ovlašćenja koja preciziraju nivoe pristupa za određene identitete. Podsystem bezbednosti servera u ovom primeru obavlja zadatak kontrole pristupa u IDA infrastrukturi.
- **Omogućava praćenje proteklih događaja** Preduzeće može poželeti da nadgleda promene na aktivnosti unutar IDA infrastrukture, tako da mora obezbediti mehanizam kojim će se upravljati praćenje.

AD DS nije jedina komponenta IDA-e koju podržava Windows Server 2008. Objavljivanjem Windows Servera 2008, Microsoft je spojio izvestan broj prethodno odvojenih komponenti u integrisanu IDA platformu. Sam aktivni direktorijum sada uključuje pet tehnologija, od kojih se svaka može identifikovati ključnom rečju, a koja identifikuje svrhu tehnologije, kao što je prikazano na slici 1-1.



**Slika 1-1** Integracija pet tehnologija aktivnog direktorijuma

Ovih pet tehnologija sačinjavaju celokupno IDA rešenje:

- **Servisi domena aktivnog direktorijuma (Identitet)** AD DS, kao što je ranije opisano, dizajniran je da obezbedi centralno spremište za upravljanje identitetom unutar organizacije. AD DS obezbeđuje servise provere identiteta i ovlašćenja u mreži i podržava upravljanje objektom kroz politiku grupe (Group Policy). AD DS takođe pruža upravljanje informacijama i deljenje servisa, omogućavajući korisnicima da pronađu bilo koju komponentu – servere datoteka, štampače, grupe i druge korisnike – pretraživanjem direktorijuma. Zbog toga AD DS se često naziva servis mrežnog operativnog sistema direktorijuma. AD DS pre svega predstavlja tehnologiju aktivnog direktorijuma i trebalo bi da bude raspoređen u svakoj mreži koja koristi Windows Server 2008 operativni sistem. O AD DS-u se govori od 1. do 13. poglavlja.

Za smernicu u kojoj su ukratko opisane najbolje vežbe za dizajniranje aktivnog direktorijuma preuzmite besplatno poglavlje 3: „Dizajniranje aktivnog direktorijuma” sa *Windows Server 2003, Best Practices for Enterprise Deployments* internet stranice [http://www.reso-net.com/Documents/007222343X\\_Ch03.pdf](http://www.reso-net.com/Documents/007222343X_Ch03.pdf).

---

**VIŠE INFORMACIJA AD DS dizajn**

Za ažurirane informacije o kreiranju dizajna servisa domena aktivnog direktorijuma, pogledajte *Windows Server 2008: The Complete Reference*, od Ruest i Ruest (McGraw-Hill Osborne, štampano izdanje).

---

- **Servisi jednostavnog direktorijuma u aktivnom direktorijumu (Aplikacije)** U suštini, samostalna verzija aktivnog direktorijuma, uloga servisa jednostavnog direktorijuma u aktivnom direktorijumu (AD LDS), ranije poznata kao režim aplikacija aktivnog direktorijuma (ADAM), pruža podršku aplikacijama podržanim od strane direktorijuma. AD LDS je zapravo podskup AD DS-a pošto se oba baziraju na istom jezgru koda. AD LDS direktorijum smešta i replicira samo informacije koje se odnose na aplikacije. Najčešće ga koriste aplikacije koje zahtevaju skladište direktorijuma, ali koje ne zahtevaju da se informacije repliciraju na nivou svih kontrolera domena. AD LDS vam takođe omogućava da rasporedite prilagođenu šemu za podršku aplikacije bez modifikovanja šeme AD DS-a. Uloga AD LDS-a je zaista jednostavna i ona podržava smeštanje više podataka u jedan sistem, tako da se svaka aplikacija može rasporediti sa sopstvenim direktorijumom, šemom, dodeljenim pristupnim protokolom jednostavnog direktorijuma (Lightweight Directory Access Protocol – LDAP), SSL portovima i dnevnikom događaja aplikacije. AD LDS se ne oslanja na AD DS, tako da se može koristiti u samostalnom okruženju ili okruženju radne grupe. Međutim, u okruženjima domena, AD LDS može koristiti AD DS za proveru identiteta Windows bezbednosnih subjekata (korisnika, grupa i računara). AD LDS se takođe može koristiti za pružanje servisa provere identiteta u izloženim mrežama kao što su spoljne mreže (extranets). Da ponovimo, korišćenjem AD LDS-a u ovoj situaciji smanjuje se rizik u odnosu na korišćenje AD DS-a. O AD LDS-u govori se u poglavlju 14.
- **Servisi sertifikata aktivnog direktorijuma (Poverenje)** Organizacije mogu koristiti servise sertifikata aktivnog direktorijuma (AD CS) kako bi podesile server sertifikata (certificate authority) za izdavanje digitalnih sertifikata kao dela infrastrukture javnih ključeva (public key infrastructure, PKI) koja povezuje identitet osobe, uređaja ili servisa sa pripadnim privatnim ključem. Sertifikati se mogu koristiti za proveru identiteta korisnika i računara, proveru baziranu na vebu, podršku provere identiteta preko pametnih kartica i za podršku aplikacija, uključujući bezbedne bežične mreže, virtuelne privatne mreže (Virtual Private Networks, VPNs), bezbednost internet protokola (Internet Protocol Security, IPSec), sistem za šifrovanje datoteka (Encrypting File System, EFS), digitalne potpise i još mnogo toga. AD CS pruža efikasan i bezbedan način za izdavanje i upravljanje sertifikatima. Možete koristiti AD CS za pružanje ovih servisa spoljašnjim zajednicama. Ako to učinite, AD CS bi trebalo da bude povezan sa spoljašnjim, čuvenim CA-om, koji će dokazati drugima da ste vi ono što tvrdite da jeste. AD CS je dizajniran za kreiranje poverenja (trust) u nepoverljivom svetu; kao takav, mora se osloniti na dokazane procese koji sertifikuju da je svaka osoba ili računar koji poseduje sertifikat pažljivo provereni i odobren. U unutrašnjim mrežama AD CS se može integrisati sa AD DS-om kako bi korisnicima i računarima automatski obezbedili sertifikate. O AD CS-u govori se u poglavlju 15.

Za više informacija o PKI infrastrukturama i o tome kako ih primeniti u vašoj organizaciji posetite internet stranicu <http://www.reso-net.com/articles.asp?m=8> i potražite odeljak „Advanced Public Key Infrastructure”.

- **Servisi upravljanja pravima aktivnog direktorijuma (Integritet)** Iako Windows koji se koristi može sprečiti ili dozvoliti pristup dokumentu na osnovu ACL-a dokumenta, postoji nekoliko načina kako bi se kontrolisalo ono što se događa dokumentu i njegovom sadržaju nakon što ga je korisnik otvorio. Servis upravljanja pravima aktivnog direktorijuma (AD RMS) predstavlja tehnologiju zaštite informacija koja vam omogućava da implementirate konstantnu upotrebu politike šablona koja definiše dozvoljenu i neautorizovanu upotrebu bilo na mreži, bilo van nje, unutar ili izvan zaštitnog zida. Na primer, mogli biste konfigurirati šablon koji korisnicima dozvoljava da čitaju dokument, ali ne i da štampaju ili kopiraju njegov sadržaj. Na taj način možete obezbediti integritet podataka koje generišete, zaštititi intelektualnu svojinu i kontrolisati ko šta može raditi sa dokumentima koje vaša organizacija pravi. AD RMS zahteva domen aktivnog direktorijuma sa kontrolerima domena koji koriste Windows 2000 Server sa servisnim paketom 3 (Service Pack 3, SP3) ili novijim; IIS; server baze podataka kao što je Microsoft SQL Server 2008; klijent AD RMS, koji možete preuzeti sa Microsoft Download Center stranice, a koji je automatski uključen u Windows Vistu i Windows Server 2008; kao i pretraživač sa aktiviranim RMS-om ili aplikaciju kao što je Microsoft Internet Explorer, Microsoft Office, Microsoft Word, Microsoft Outlook ili Microsoft PowerPoint. AD RMS se može osloniti na AD CS kako bi se u dokumente ugradili sertifikati, kao i na AD DS kako bi se upravljalo pravima pristupa. O AD RMS-u govori se u poglavlju 16.
- **Servisi ujedinjenja aktivnog direktorijuma (Partnerstvo)** Servis ujedinjenja aktivnog direktorijuma (AD FS) omogućava da organizacija proširi IDA-u kroz više platformi, uključujući i Windows okruženja i ona koja ne koriste Windows, kao i da projektuje identitet i prava pristupa kroz granice bezbednosti za partnere od poverenja. U ujedinjenom okruženju svaka organizacija održava i upravlja sopstvenim identitetima, ali ona takođe sa sigurnošću može projektovati i prihvatiti identitete i iz drugih organizacija. Proverava se identitet korisnika u jednoj mreži, ali on može pristupiti resursima i u nekoj drugoj mreži – ovaj proces je poznat kao jednokratno prijavljivanje (Single Sign-on, SSO). AD FS podržava partnerstva zato što dozvoljava da različite organizacije dele pristup spoljnim aplikacijama dok se oslanjaju na sopstvene unutrašnje AD DS strukture kako bi izvršile proces stvarne provere identiteta. Da bi to uradile, AD FS proširuje vašu unutrašnju AD DS strukturu na spoljašnji svet kroz zajedničke portove protokola za kontrolu prenosa/internet protokola (Transmission Control Protocol/Internet Protocol), kao što su portovi 80 (HTTP) i 443 (bezbedni HTTP ili HTTPS). Najčešće se nalazi u tampon zoni (perimeter network, buffer zone). AD FS se može osloniti na AD CS kako bi se kreirali poverenički serveri, kao i na AD RMS kako bi se obezbedila spoljašnja zaštita celokupne intelektualne svojine. O AD FS-u govori se u poglavlju 17.

Uloge aktivnog direktorijuma zajedno daju integrisano IDA rešenje. AD DS ili AD LDS obezbeđuje osnovne servise direktorijuma i u domenu i u samostalnim implementacijama. AD CS obezbeđuje identifikatore od poverenja u obliku PKI digitalnih sertifikata. AD RMS štiti integritet informacija sadržanih u dokumentima. I na kraju, AD FS podržava partnerstva eliminisanjem potrebe da ujedinjena okruženja kreiraju više odvojenih identiteta za jedan bezbedonosni subjekt.

## Posle identiteta i pristupa

Aktivni direktorijum ne pruža samo IDA rešenja. Naprotiv, on takođe obezbeđuje mehanizme za podršku, upravljanje i konfigurisanje resursa u distribuiranim mrežnim okruženjima.

Skup pravila, odnosno *šema (schema)*, definiše klase objekata i atributa koji mogu biti sadržani u direktorijumu. Činjenica je da aktivni direktorijum sadrži korisničke objekte koji uključuju korisničko ime i lozinku, i to se dešava zbog toga što šema definiše klasu *korisničkog objekta (user object class)*, dva atributa i asocijaciju između klase objekta i atributa.

Administracija na bazi politike olakšava teret upravljanja čak i najvećim, najsloženijim mrežama tako što obezbeđuje jedno mesto na kome će se konfigurisati podešavanja koja se potom raspoređuju u više sistema. O ovim politikama, uključujući i politiku grupe (*group policy*), politiku nadgledanja događaja i politike lozinke visoke rezolucije, učićete u poglavlju 6 „Infrastruktura politike grupe”, 7 – „Podešavanja politike grupe” i u poglavlju 8.

Servisi replikacije distribuiraju podatke direktorijuma kroz mrežu. Ovo uključuje i skladište podataka, a i podatke neophodne za implementaciju politika i konfiguracije, uključujući i prijavne skriptove. U poglavlju 8, poglavlju 11 „Lokacije i replikacija” i poglavlju 10, učićete o replikaciji aktivnog direktorijuma. Postoji čak i odvojena particija skladišta podataka pod nazivom *konfiguracija (configuration)*, koja vodi računa o informacijama koje se tiču konfiguracije mreže, topologije i servisa.

Nekoliko komponenti i tehnologija omogućavaju vam da upitate aktivni direktorijum i pronađete objekte u skladištu podataka. Particija skladišta podataka pod nazivom *globalni katalog (Global Catalog)* (takođe poznat kao *delimični skup atributa – Partial Attribute Set*) sadrži informacije o svakom objektu u direktorijumu. To je neka vrsta indeksa koji se može koristiti za pronalaženje objekata u direktorijumu. Programska okruženja kao što su okruženje servisa aktivnog direktorijuma (*Active Directory Services Interface, ADSI*) i protokoli poput LDAP-a, mogu se koristiti za čitanje i manipulisanje skladištem podataka.

Skladište podataka aktivnog direktorijuma takođe se može koristiti za podršku aplikacija i servisa koji nisu direktno povezani sa AD DS-om. Unutar baze podataka, particije aplikacija mogu smestiti podatke za podršku aplikacija koje zahtevaju replicirane podatke. Servis sistema imenovanja domena (*Domain Name System, DNS*) može na serveru koji koristi Windows Server 2008 smestiti svoje informacije u bazi podataka pod nazivom integrisana zona aktivnog direktorijuma (*Active Directory Integrated Zone*), a koja se održava kao particija aplikacije u AD DS-u i replicira korišćenjem servisa replikacije aktivnog direktorijuma.

## Komponente infrastrukture aktivnog direktorijuma

Prvih 13 poglavlja ovog udžbenika za pripremu ispita fokusira se na instalaciju, konfiguraciju i upravljanje AD DS-om. AD DS predstavlja osnovu za IDA-u u mreži preduzeća i upravljanje istom. Vredi provesti nekoliko minuta u obnavljanju komponenti infrastrukture aktivnog direktorijuma.



---

**NAPOMENA** Gde pronaći detalje o aktivnom direktorijumu

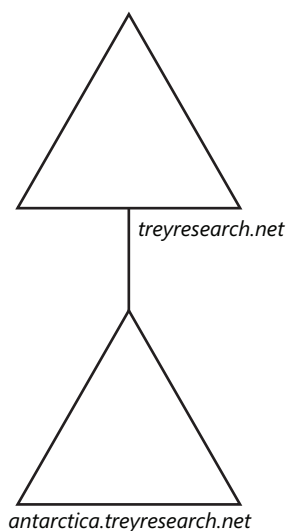
Za više detalja o aktivnom direktorijumu pogledajte pomoć o proizvodu koja je instalirana sa Windows Serverom 2008 i TechCenter za Windows Server 2008 na internet lokaciji <http://technet.microsoft.com/en-us/windowsserver/2008/default.aspx>.

---

- **Skladište podataka aktivnog direktorijuma** Kao što je napomenuto u prethodnom odeljku, AD DS smešta svoje identitete u direktorijum – skladište podataka koje se čuva na kontrolerima domena. Direktorijum je datoteka pod nazivom Ntds.dit i podrazumevano se nalazi u fascikli %SystemRoot%\Ntds na kontroleru domena. Baza podataka je podeljena na nekoliko particija, uključujući šemu, konfiguraciju, globalni katalog i domen koji označava kontekst koji sadrži podatke o objektima unutar domena, na primer, korisnicima, grupama i računarima.
- **Kontroleri domena** Kontroleri domena, skraćeno nazvani DC-i (DCs), jesu serveri koji obavljaju AD DS ulogu. Kao deo uloge, oni takođe vrše servis Kerberosovog centra za distribuciju ključeva (Kerberos Key Distribution Center, KDC), koji obavlja proveru identiteta i druge servise aktivnog direktorijuma. U poglavlju 10 detaljnije se opisuju uloge koje obavljaju DC-i.
- **Domen** Potreban je jedan ili više kontrolera domena kako bi se kreirao *domen* (*Domain*) aktivnog direktorijuma. Domen je administrativna jedinica unutar koje se dele određene mogućnosti i karakteristike. Prvo, svi kontroleri domena repliciraju particiju skladišta podataka domena koja, između ostalog, sadrži identitet podataka za korisnike, grupe i računare. Pošto svi DC-i održavaju isto skladište identiteta, bilo koji DC može proveriti bilo koji identitet u domenu. Osim toga, domen predstavlja i oblast administrativnih politika, kao što su politike složenosti lozinke i isključenja naloga. Ove politike, koje su konfigurisane u jednom domenu, utiču na sve naloge u njemu, ali ne i na naloge u drugim domenima. Bilo koji kontroler domena može napraviti promene na objektima u bazi podataka aktivnog direktorijuma i one se mogu replicirati na sve ostale kontrolere domena. Prema tome, u mrežama u kojima se replikacija svih podataka među kontrolerima domena ne može podržati, možda će biti neophodno implementirati više od jednog domena da bi se upravljalo replikacijom podskupova identiteta. Više o domenima saznaćete u poglavlju 12.
- **Šuma** *Šuma* (*forest*) predstavlja kolekciju jednog ili više domena aktivnog direktorijuma. Prvi domen instaliran u šumi naziva se *osnovni domen šume* (*Forest Root Domain*). Šuma sadrži jednu definiciju konfiguracije mreže i jednu instancu šeme direktorijuma. Šuma predstavlja jednu instancu direktorijuma – nijedan podatak se ne replicira od strane aktivnog direktorijuma izvan granica šume. Dakle, šuma definiše granicu bezbednosti. Koncept šume detaljnije se istražuje u poglavlju 12.
- **Stablo** DNS imenski prostor domena u šumi kreira stabla unutar šume. Ukoliko domen predstavlja poddomen nekog drugog domena, ta dva domena se smatraju stablom. Na primer, ukoliko *tresearch.net* šuma sadrži dva domena, domene *tresearch.net* i *antarctica.tresearch.net*, oni prave susedni deo DNS imenskog prostora, pa se nalaze u jednom stablu. Ukoliko su, međutim, ta dva domena *tresearch.net* i

*proseware.com*, koji nisu susedni u DNS imenskom prostoru, smatra se da domen ima dva stabla. Stabla predstavljaju direktan rezultat DNS imena izabranih za domene u šumi.

Slika 1-2 ilustruje šumu aktivnog direktorijuma za domen Trey Research, koji obavlja sitnu operaciju na stanici na Antarktiku. Pošto je veza od Antarktiku do sedišta firme skupa, spora i nepouzdana, domen na Antarktiku je konfigurisan kao odvojen domen. DNS ime šume je *treyresearch.net*. Domen Antartica je domen potomak u DNS imenskom prostoru, tj. *antarctica.treyresearch.net*, pa se zbog toga smatra domenom potomkom u stablu domena.



**Slika 1-2** Šuma aktivnog direktorijuma sa dva domena

- Funkcionalni nivo** Funkcionalnost dostupna u domenu ili šumi aktivnog direktorijuma zavisi od njenog *funkcionalnog nivoa* (*Functional Level*). Funkcionalni nivo je AD DS podešavanje koje aktivira napredne AD DS karakteristike na nivou domena ili šume. Postoje tri funkcionalna nivoa domena: početni Windows 2000 (Windows 2000 Native), Windows Server 2003 i Windows Server 2008, kao i dva funkcionalna nivoa šume: Microsoft Windows Server 2003 i Windows Server 2008. Kako podižete funkcionalni nivo domena ili šume, karakteristike date u toj verziji Windowsa postaju dostupne AD DS-u. Na primer, kada je funkcionalni nivo domena podignut na Windows Server 2008, nov atribut postaje dostupan i on otkriva kada se korisnik poslednji put uspešno prijavio na računar, zatim na koji se računar korisnik poslednji put prijavio, kao i broj neuspešnih pokušaja prijave od poslednje prijave. Bitna stvar koju treba znati u vezi sa funkcionalnim nivoima jeste ta što oni određuju koje su verzije Windowsa dozvoljene na kontrolerima domena. Pre nego što podignete funkcionalni nivo domena na Windows Server 2008, svi kontroleri domena moraju koristiti Windows Server 2008. Funkcionalni nivoi domena i šume detaljnije su opisani u poglavlju 12.

- **Organizacione jedinice** Aktivni direktorijum predstavlja hijerarhijsku bazu podataka. Objekti u skladištu podataka mogu se sakupljati u kontejnerima. Jedna vrsta kontejnera predstavlja klasu objekta pod nazivom *kontejner (container)*. Kada otvorište modul Active Directory Users and Computers, vidite podrazumevane kontejnere, uključujući i kontejnere Users, Computers i Builtin. Još jedna vrsta kontejnera je i organizaciona jedinica (organizational unit, OU). OU-i snabdevaju objekte ne samo kontejnerom već i izvesnim opsegom kojim se njima upravlja. Ovo se dešava zbog toga što OU-i mogu sadržati objekte koji se nazivaju objekti politike grupe (Group Policy Objects, GPOs) i koji su povezani sa OU-ima. GPO-i mogu sadržati podešavanja konfiguracije, koja će potom automatski biti primenjena u jednoj OU od strane korisnika ili računara. O OU-ima ćete više naučiti u poglavlju 2 „Administracija”, a u poglavlju 6 ćete istražiti GPO-e.
- **Lokacije** Kada uzmete u obzir topologiju mreže raspodeljenog preduzeća, sigurno ćete diskutovati o lokacijama mreže. Lokacije u aktivnom direktorijumu, međutim, imaju veoma specifično značenje zato što postoji određena klasa objekta koja se naziva *lokacija (site)*. Lokacija aktivnog direktorijuma je objekat koji predstavlja deo preduzeća unutar koga je mrežna povezanost dobra. Lokacija kreira granicu replikacije korišćenja servisa. Kontroleri domena unutar jedne lokacije repliciraju promene u roku od nekoliko sekundi. Promene se na kontrolisanoj bazi repliciraju između lokacija uz pretpostavku da su veze između lokacija spore, skupe ili nepouzdana u poređenju sa vezama unutar jedne lokacije. Osim toga, klijenti će više voleti da koriste distribuirane servise koje serveri pružaju na njihovoj lokaciji ili najbližoj lokaciji. Na primer, kada se korisnik prijavi na domen, Windows klijent najpre pokušava da proveri identitet pomoću kontrolera domena na njegovoj lokaciji. Samo u slučaju da kontroler domena nije dostupan na lokaciji, klijent će pokušati da proveri identitet pomoću DC-a na nekoj drugoj lokaciji. Konfiguracija i funkcionalnost lokacija aktivnog direktorijuma detaljnije su opisane u poglavlju 11.

O svakoj od ovih komponenti detaljno se će se raspravljati kasnije u ovom udžbeniku za pripremu ispita. U ovom trenutku, ukoliko ne poznajete dovoljno aktivni direktorijum, važno je da imate samo osnovno razumevanje terminologije, komponenti i njihovih odnosa.

## Priprema za kreiranje nove šume Windows Servera 2008

Pre nego što na server instalirate AD DS ulogu i promovišete je kako bi delovala kao kontroler domena, isplanirajte vašu infrastrukturu aktivnog direktorijuma. Neke od informacija koje će vam biti potrebne za kreiranje kontrolera domena uključuju sledeće:

- Ime domena i DNS ime. Domen mora imati jedinstveno DNS ime, na primer *contoso.com*, kao i kratko ime, na primer CONTOSO, koje je NetBIOS ime. NetBIOS je protokol koji se koristi od prvih verzija Microsoft Windowsa NT i koji još uvek koriste neke aplikacije.
- Da li će biti potrebno da domen podrži kontrolere domena koji koriste prethodne verzije Windowsa. Kada kreirate novu šumu aktivnog direktorijuma, konfigurisaćete funkcionalni nivo. Ukoliko će domen uključivati samo kontrolere domena Windows

Servera 2008, možete podesiti funkcionalni nivo na osnovu prednosti dobijene od poboljšanih karakteristika predstavljenih u ovoj verziji Windowsa.

- Detalje o tome kako će DNS biti implementiran za podršku aktivnog direktorijuma. Najbolje je implementirati DNS za vaše zone domena Windowsa tako što ćete koristiti Windows DNS servis (Windows DNS Service), o čemu ćete učiti u poglavlju 9 „Integrisanje sistema imenovanja domena pomoću AD DS-a”; međutim, moguće je podržati Windows domen na DNS rešenju drugog proizvođača.
- IP konfiguraciju za kontroler domena. Kontroleri domena zahtevaju statičke IP adrese i vrednosti maske podmreže. Osim toga, kontroler domena se mora konfigurisati adresom DNS servera kako bi se izvelo razrešavanje imena. Ukoliko ćete kreirati novu šumu i koristiti Windows DNS servis (Windows DNS Service) na kontroleru domena, možete konfigurisati da se DNS adresa usmeri na IP adresu samog servera. Nakon instaliranja DNS-a server može sam razrešavati DNS imena.
- Korisničko ime i lozinku naloga u grupi servera Administrators. Nalog mora posedovati lozinku – ona ne može biti prazna.
- Lokaciju na kojoj bi skladište podataka (uključujući i *Ntds.dit*) i sistemski disk (SYSVOL) trebalo da budu instalirani. Podrazumeva se da su ova skladišta kreirana u fascikli %SystemRoot%, kao što je, na primer C:\Windows, u odgovarajućim fasciklama NTDS i SYSVOL. Prilikom kreiranja kontrolera domena ova skladišta možete preusmeriti na druge jedinice diska.

---

#### VIŠE INFORMACIJA    Raspoređivanje AD DS-a

Ova lista obuhvata podešavanja za čiju konfiguraciju će se pojaviti prozori prilikom kreiranja kontrolera domena. Postoji izvestan broj dodatnih razmatranja koja se odnose na AD DS raspored u podešavanju preduzeća. Za više informacija pogledajte Windows Server 2008 Technical Library na internet stranici <http://technet2.microsoft.com/windowsserver2008/en/library/bab0f1a1-54aa-4cef-9164-139e8bcc44751033.msp>.

---

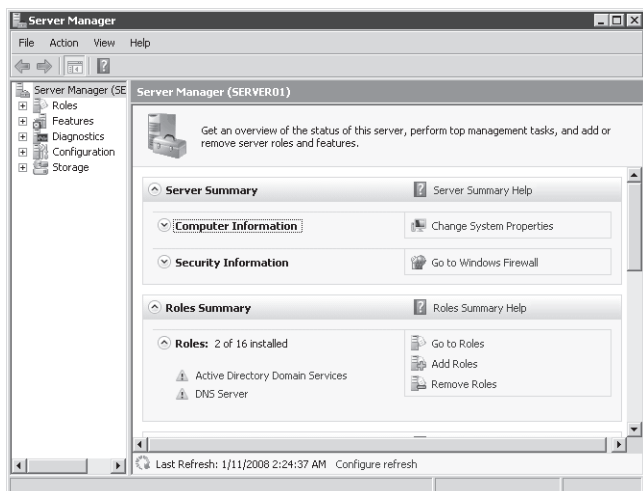
## Dodavanje AD DS uloge korišćenjem Windows okruženja

Nakon što ste prikupili najbitnije informacije koje su ranije izlistane, spremni ste da dodate AD DS ulogu. Postoji nekoliko načina da to uradite. U ovoj lekciji naučićete kako da kreirate kontroler domena koristeći Windows okruženje. U narednoj lekciji to ćete naučiti tako što ćete koristiti komandnu liniju.

Windows Server 2008 obezbeđuje konfiguraciju zasnovanu na ulozi, instaliranjem samo onih komponenti i servisa koji su potrebni za uloge koje server igra. Ovo upravljanje serverom na bazi uloge ispoljava se u administrativnoj konzoli Server Manager, koja je prikazana na slici 1-3. Server Manager konsoliduje informacije, alatke i resurse potrebne za podršku uloga servera.

Serveru možete dodati uloge koristeći vezu Add Roles na početnoj strani konzole Server Manager ili pritiskom desnog tastera miša na čvor Roles u stablu konzole i biranjem opcije

Add Roles. Čarobnjak za dodavanje uloga (Add Roles Wizard) prikazuje listu uloga dostupnih za instaliranje i postepeno vas vodi kroz instalaciju izabranih uloga.



Slika 1-3 Server Manager

---

**Vežbajte** Vežbanje 3 „Instalirajte novu šumu Windows Servera 2008 pomoću Windows okruženja“ na kraju ove lekcije vodi vas kroz proces dodavanja AD DS uloge korišćenjem Windows okruženja.

---

## Kreiranje kontrolera domena

Nakon što dodate AD DS ulogu, datoteke potrebne za obavljanje te uloge instalirane su na serveru, ali server još uvek ne funkcioniše kao kontroler domena. Zato morate otvoriti čarobnjaka za instalaciju servisa domena aktivnog direktorijuma (Active Directory Domain Services Installation Wizard), koji se može pokrenuti korišćenjem komande *Dcpromo.exe* kako biste konfigurisali, inicijalizovali i pokrenuli aktivni direktorijum.

---

**Vežbajte** Vežbanje 4 „Instalirajte novu šumu Windows Servera 2008“ na kraju ove lekcije vodi vas kroz proces konfiguracije AD DS-a korišćenjem čarobnjaka za instalaciju servisa domena aktivnog direktorijuma.

---

### Brza provera

- Želite da upotrebite nov server koji koristi Windows Server 2008 kao kontroler domena u vašem domenu aktivnog direktorijuma. Koju ćete komandu koristiti kako biste pokrenuli konfiguraciju kontrolera domena?

### Odgovor brze provere

- *Dcpromo.exe*.

## VEŽBA    Kreiranje šume Windows Servera 2008

U ovoj vežbi kreiraćete AD DS šumu za Contoso, Ltd. Ova šuma će se koristiti u vežbanjima kroz ceo ovaj udžbenik za pripremu ispita. Počecete instaliranjem Windows Servera 2008 i obavljanjem zadatka konfiguracije nakon instalacije. Potom ćete dodati AD DS ulogu i unaprediti server u kontroler domena u šumi *contoso.com* korišćenjem čarobnjaka za instalaciju servisa domena aktivnog direktorijuma.

### ► Vežbanje 1    Instalirajte Windows Server 2008

U ovom vežbanju instaliraćete Windows Server 2008 na računar ili virtuelnu mašinu.

#### 1. Ubacite Windows Server 2008 instalacioni DVD.

Ako koristite virtuelnu mašinu (VM), možda ćete imati opciju da postavite ISO sliku instalacionog DVD-a. Konsultujte VM Help dokumentaciju za uputstva.

#### 2. Uključite sistem.

Ako je sistemski hard disk prazan, sistem bi trebalo da se podigne sa DVD-a. Ukoliko se na disku nalaze podaci, možda će se pojaviti poruka koja vam upućuje da pritisnete neki taster kako biste podigli sistem sa DVD-a.

Ako se sistem ne podigne preko DVD-a ili vam ne ponudi meni za podizanje sistema, otvorite BIOS podešavanja računara i konfigurirate redosled podizanja sistema kako biste bili sigurni da se sistem podiže sa DVD-a.

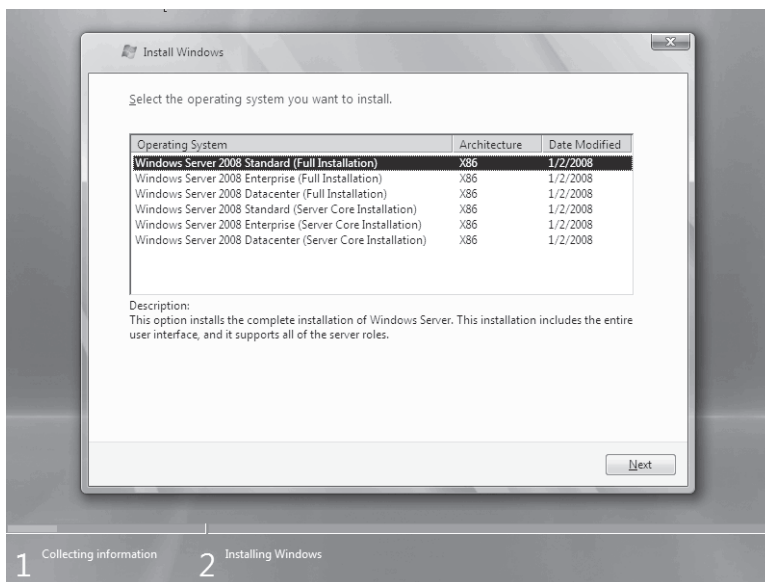
Pojaviće se čarobnjak za instalaciju Windowsa (Install Windows Wizard), koji je prikazan na slici 1-4.



**Slika 1-4**    Install Windows Wizard

3. Izaberite jezik, regionalno podešavanje i raspored tastera na tastaturi koji odgovaraju vašem sistemu, pa pritisnite Next.
4. Pritisnite Install Now.

Prikazaće vam se lista verzija za instaliranje, kao što je prikazano na slici 1-5. Ukoliko koristite x64 računar, prikazaće vam se x64 verzije, a ne x86 verzije.

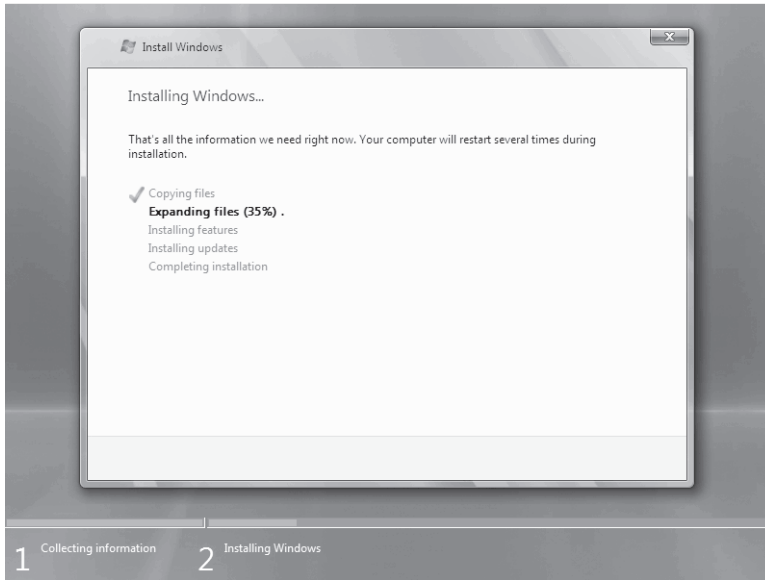


**Slika 1-5** Strana Select The Operating System You Want To Install

5. Izaberite Windows Server 2008 Standard (Full Installation), pa pritisnite Next.
6. Izaberite polje za potvrdu I Accept The Licence Terms pa pritisnite Next.
7. Pritisnite Custom (Advanced).
8. Na strani Where Do You Want to Install Windows izaberite disk na koji želite da instalirate Windows Server 2008.  
Ukoliko je potrebno da kreirate, obrišete, proširite ili formatirate particije ili ukoliko je potrebno da učitate prilagođeni upravljački program velikog skladišta kako biste pristupili podsistemu diska, pritisnite Driver Options (Advanced).
9. Pritisnite Next.

Pojavljuje se okvir za dijalog Installing Windows, koji je prikazan na slici 1-6. Prozor vas stalno obaveštava o napretku instalacije Windowsa.

Instalacija Windows Servera 2008, poput one za Windows Vistu, zasniva se na slici (image-based). Zbog toga je instalacija znatno brža od one za ranije verzije Windowsa iako su sami operativni sistemi mnogi veći od ranijih verzija. Računar će se ponovno pokrenuti jednom ili više puta tokom instalacije.



**Slika 1-6** Strana Installing Windows

Kada se instalacija završi, bićete informisani o tome da se lozinka korisnika mora promeniti pre prvog prijavlivanja.

10. Pritisnite OK.
11. Ukucajte lozinku za nalog Administrator i u polju New Password i u polju Confirm Password, pa pritisnite Enter.

Lozinka se mora sastojati od najmanje sedam karaktera i imati barem tri ili četiri vrste karaktera:

- Veliko slovo: A – Z
- Malo slovo: a – z
- Broj: 0 – 9
- Simbole koji nisu ni slova ni brojevi, poput \$, #, @ i !

---

**NAPOMENA** Nemojte zaboraviti ovu lozinku

Bez nje nećete moći da se prijavite na server kako biste uradili ostala vežbanja u ovom udžbeniku za pripremu ispita.

---

12. Pritisnite OK.
- Pojavljuje se radna površina naloga Administrator.

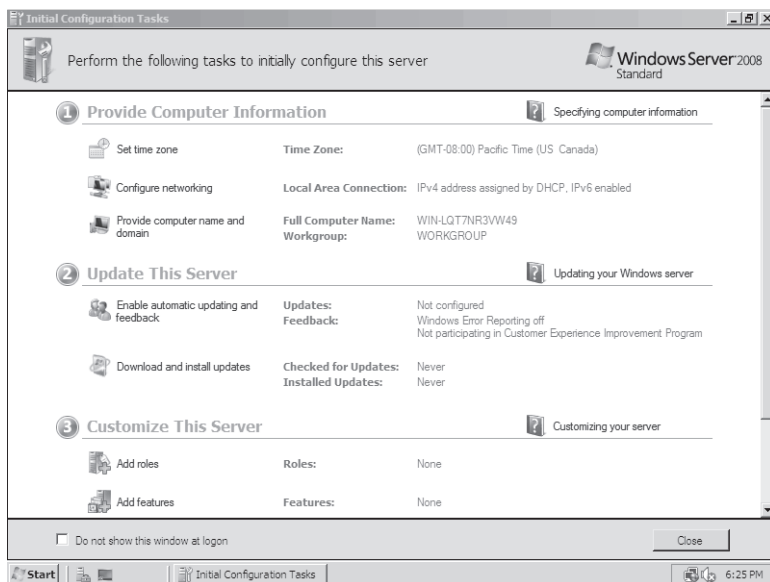


## ► Vežbanje 2 Izvršite konfiguraciju nakon instalacije

U ovom vežbanju nakon završene instalacije konfigurisaćete server kako biste pripremili server sa imenom i TCP/IP podešavanjima za vežbanja u ovom udžbeniku za pripremu ispita.

1. Sačekajte da se na radnoj površini pojavi nalog Administrator.

Pojavljuje se prozor Initial Configuration Tasks, kao što je prikazano na slici 1-7. Ova alatka je dizajnirana kako bi vam olakšala da na najbolji način provežbate zadatke konfiguracije nakon instalacije.



**Slika 1-7** Prozor Initial Configuration Tasks

2. Koristite prozor Initial Configuration Tasks kako biste konfigurisali sledeća podešavanja:
  - Vremensku zonu: podesite je prema vašem okruženju.
  - Naziv računara: SERVER01. Nemojte ponovo pokretati sistem dok ne dobijete instrukcije da to uradite kasnije u ovom vežbanju.
3. Pritisnite na vezu Configure Networking u prozoru Initial Configuration Tasks i proverite da li IP konfiguracija servera odgovara vašem okruženju.
4. Ukoliko je server povezan sa internetom, vrlo je preporučljivo da pritisnete vezu Download And Install Updates kako biste mogli da ažurirate server sa poslednjim verzijama za bezbednost koje pruža Microsoft.
5. Nakon ažuriranja servera ponovo pokrenite server.

Preostala vežbanja u ovom udžbeniku za pripremu ispita kreirace domen korišćenjem IP adresa u rasponu od 10.0.0.11 do 10.0.0.20, sa maskom pod mreže 255.255.255.0. Ukoliko se ove adrese koriste u vašem proizvodnom okruženju i ukoliko je server

povezan na vaše proizvodno okruženje, morate onda promeniti IP adrese i u ovoj knjizi, tako da se *contoso.com* domen koji kreirate u ovim vežbanjima ne sukobljava sa vašom proizvodnom mrežom.

6. U prozoru Initial Configuration Tasks pritisnite na vezu Configure Networking. Pojavljuje se okvir za dijalog Network Connections.
7. Izaberite Local Area Connection.
8. Na liniji sa alatkama pritisnite Change Settings Of This Connection.
9. Izaberite Internet Protocol Version 4 (TCP/IPv4), pa pritisnite Properties. Windows Server 2008 takođe pruža podršku za Internet Protocol Version 6 (TCP/IPv6).
10. Pritisnite Use The Following IP Address. Unesite sledeću konfiguraciju:
  - IP adresa: 10.0.0.11
  - Maska podmreže: 255.255.255.0
  - Podrazumevani mrežni prolaz: 10.0.0.1
  - Preferirani DNS server: 10.0.0.11

11. Pritisnite OK, a zatim Close.

12. Obratite pažnju na veze Add Roles i Add Features u prozoru Initial Configuration Tasks.

U sledećem vežbanju koristićete Server Manager kako biste dodali uloge i karakteristike serveru SERVER01. Ove veze predstavljaju još jedan način da bi se izveli isti zadaci.

Prozor Initial Configuration Tasks će se pojaviti svaki put kada se prijavite na server.

13. Izaberite polje za potvrdu Do Not Show This Window At Logon kako biste sprečili da se prozor ponovo pojavljuje.

Ukoliko je potrebno da ubuduće otvarate prozor Initial Configuration Tasks, to ćete uraditi tako što ćete aktivirati komandu *Oobe.exe*.

14. Pritisnite dugme Close na dnu prozora Initial Configuration Tasks. Pojaviće se Server Manager. Server Manager vam omogućava da konfigurišete i administrirate uloge i karakteristike servera koji koristi Windows Server 2008. Koristićete Server Manager u sledećem vežbanju.

---

#### **NAPOMENA    Napravite snimak (snapshot) vaše virtuelne mašine**

Ukoliko koristite virtuelnu mašinu da biste uradili ovo vežbanje i ukoliko vam ona omogućava da napravite snimke stanja mašine u određenom trenutku, učinite to sada. Ova osnovna instalacija Windows Servera 2008 može se koristiti kako biste uradili vežbanja u ovom poglavlju, koja vam daju mogućnost da eksperimentišete sa raznovrsnim metodama dodavanja AD DS uloge.

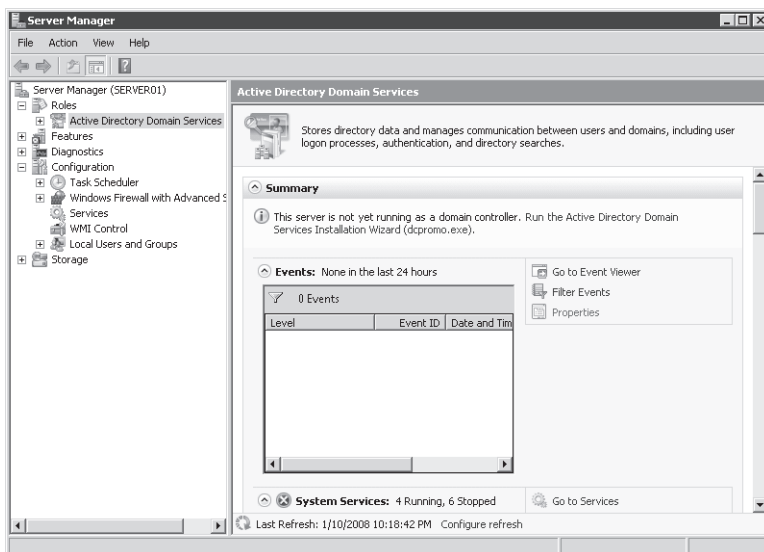
---

**► Vežbanje 3 Instalirajte novu šumu Windows Servera 2008 pomoću Windows okruženja**

U ovom vežbanju dodaćete AD DS ulogu serveru koji ste instalirali i konfigurisali u vežbanju 1 „Instalirajte Windows Server 2008” i vežbanju 2 „Izvršite konfiguraciju nakon instalacije”.

1. Ukoliko Server Manager nije otvoren, otvorite ga iz programske grupe Administrative Tools.
2. U odeljku Roles Summary na početnoj strani pritisnite Add Roles. Pojavljuje se prozor Add Roles Wizard.
3. Pritisnite Next.
4. Na strani Select Server Roles izaberite polje za potvrdu koje se nalazi pored odeljka Active Directory Domain Services. Pritisnite Next.
5. Na strani Active Directory Domain Services pritisite Next.
6. Na strani Confirm Installation Selections pritisnite Install.  
Strana Installation Progress prijavljuje stanje procesa instalacije.
7. Na strani Installation Results potvrdite da je instalacija uspešno završena, pa pritisnite Close.

U odeljku Roles Summary na početnoj strani konzole Server Manager primetićete poruku o grešci označenu crvenim kružićem sa belim krstićem (x). Na strani ćete takođe primetiti poruku i u odeljku Active Directory Domain Services. Obe ove veze će vas uputiti na stranu uloge Active Directory Domain Services u konzoli Server Manager, koja je prikazana na slici 1-8. Prikazana poruka vas podseća da je neophodno da pokrenete *Dcpromo.exe*, što ćete uraditi u narednom vežbanju.



**Slika 1-8** Strana uloga Active Directory Domain Services u prozoru Server Manager

## ► Vežbanje 4    Instalirajte novu šumu Windows Servera 2008

U ovom vežbanju koristit ćete Active Directory Domain Services Installation Wizard (*Dcpromo.exe*) kako biste kreirali novu šumu Windows Servera 2008.

1. Pritisnite Start, zatim Run, ukucajte **Dcpromo.exe**, pa onda pritisnite OK.

---

### **NAPOMENA**    Dcpromo će dodati AD DS ulogu ukoliko je neophodno

U prethodnom vežbanju dodali ste AD DS ulogu korišćenjem konzole Server Manager. Međutim, ukoliko pokrenete *Dcpromo.exe* na serveru na kome još uvek nije instalirana AD DS uloga, *Dcpromo.exe* će je automatski instalirati.

---

Pojavljuje se prozor Active Directory Domain Installation Wizard. U poglavlju 10 naučićete više o naprednim režimima ovog čarobnjaka.

2. Pritisnite Next.
3. Na strani Operating System Compatibility pregledajte upozorenje o podrazumevanim sigurnosnim podešavanjima za kontrolere domena Windows Servera 2008, pa potom pritisnite Next.
4. Na strani Choose a Deployment Configuration izaberite Create A New Domain In A New Forest, pa pritisnite Next.
5. Na strani Name The Forest Root Domain ukucajte **contoso.com**, pa pritisnite Next.  
Sistem vrši proveru kako bi proverio da DNS i NetBIOS imena nisu već u upotrebi na mreži.
6. Na strani Set Forest Functional Level izaberite Windows Server 2008, pa pritisnite Next.

Svaki od funkcionalnih nivoa je na strani opisan u polju Details. Biranjem funkcionalnog nivoa šume Windows Servera 2008 obezbeđuje se da svi domeni u šumi rade na funkcionalnom nivou domena Windows Servera 2008, koji aktivira nekoliko novih karakteristika koje daje Windows Server 2008. O funkcionalnim nivoima učićete u poglavlju 12.

Pojavljuje se strana Additional Domain Controller Options. Podrazumeva se da je izabran DNS Server. Active Directory Domain Services Wizard će kreirati DNS infrastrukturu tokom AD DS instalacije. Prvi kontroler domena u šumi mora biti server globalnog kataloga (GC) i ne može biti kontroler domena sa pravima čitanja (RODC).

7. Pritisnite Next.  
Pojavljuje se upozorenje za dodeljivanje statičkog IP-a (Static IP assignment). Pošto se u ovom udžbeniku za pripremu ispita ne govori o IPv6 adresi, u vežbanju 2 serveru niste dodelili statičku IPv6 adresu. Dodelili ste statičku IPv4 adresu u tom vežbanju, pa će se i u narednim vežbanjima koristiti IPv4. Zbog toga možete ignorisati ovo upozorenje u okviru ovog vežbanja.
8. Pritisnite Yes, The Computer Will Use A Dynamically Assigned IP Address (Not Recommended).

Pojavljuje se upozorenje koje vas informiše o tome da se delegacija za DNS server ne može kreirati. U okviru ovog vežbanja možete ignorisati ovu grešku. O delegacijama DNS domena govoriće se u poglavlju 9.

9. Pritisnite Yes kako biste zatvorili Active Directory Domain Services Wizard poruku o upozorenju.
10. Na strani Location For Database, Log Files, And SYSVOL, prihvatite podrazumevane lokacije za datoteku baze podataka, datoteke evidencije servisa direktorijuma i datoteke SYSVOL, pa pritisnite Next.

U proizvodnom okruženju najbolje bi bilo da ove datoteke smestite na tri različite jedinice diska koje ne sadrže aplikacije ili druge datoteke koje se ne odnose na AD DS. Ovakva praksa poboljšava rad i povećava efikasnost izrađivanja rezervne kopije i restauracije.

11. Na strani Directory Services Restore Mode Administrator Password ukucajte jaku lozinku u poljima Password i Confirmed Password. Pritisnite Next.

Nemojte zaboraviti lozinku koju ste dodelili administratoru za režim vraćanja servisa direktorijuma (Directory Services Restore Mode Administrator).

12. Na strani Summary pregledajte svoje odabire.

Ako je bilo koje podešavanje neispravno, pritisnite Back kako biste uneli modifikacije.

13. Pritisnite Next.

Počinje konfiguracija AD DS-a. Server će zahtevati ponovno pokretanje kada se proces završi. Ako želite, izaberite polje za potvrdu Reboot On Completion.

## Pregled lekcije

- Servisi aktivnog direktorijuma obuhvataju integrisano rešenje za identitet i pristup mrežama preduzeća.
- Servisi domena aktivnog direktorijuma (Active Directory Domain Services, AD DS) obezbeđuju servis direktorijuma i IDA komponente provere identiteta. Osim toga, AD DS olakšava upravljanje još većim i složenijim distribuiranim mrežama.
- Windows Server 2008 sistemi konfigurisani su na osnovu uloga koje obavljaju. Možete dodati AD DS ulogu korišćenjem konzole Server Manager.
- Koristite *Dcpromo.exe* kako biste konfigurisali AD DS i kreirali kontroler domena.

## Obnavljanje lekcije

Možete koristiti sledeća pitanja kako biste proverili svoje znanje o informacijama u lekciji 1 „Instaliranje servisa aktivnog direktorijuma”. Pitanja su takođe dostupna na prapratnom CD-u ukoliko preferirate da ih pregledate u elektronskoj formi.

**NAPOMENA    Odgovori**

Odgovori na ova pitanja i objašnjenja o tome zašto je svaki izbor odgovora tačan ili netačan nalaze se u odeljku „Odgovori“ na kraju knjige.

---

1. Šta je od sledećeg potrebno kako bi se uspešno kreirao kontroler domena? (Izaberite sve što je moguće.)
  - A. Validno ime DNS domena.
  - B. Validno NetBIOS ime.
  - C. DHCP server za dodelu IP adrese kontroleru domena.
  - D. DNS server.
  
2. Trey Research je nedavno nabavio Litware, Inc. Zbog pitanja o regularnosti koja se odnosi na replikaciju podataka, odlučeno je da se konfiguriše domen potomak u šumi za korisnike i računare u Litwareu. Šuma Trey Research trenutno sadrži samo kontrolere domena Windows Servera 2008. Nov domen će se kreirati promovisanjem kontrolera domena Windows Servera 2008, ali će možda biti potrebno da koristite postojeće Windows Server 2003 sisteme kao kontrolere domena u domenu Litware. Koji će funkcionalni nivoi biti pogodni da se konfigurišu?
  - A. Funkcionalni nivo šume Windows Servera 2008 i funkcionalni nivo domena Windows Servera 2008 za domen Litware.
  - B. Funkcionalni nivo šume Windows Servera 2008 i funkcionalni nivo domena Windows Servera 2003 za domen Litware.
  - C. Funkcionalni nivo šume Windows Servera 2003 i funkcionalni nivo domena Windows Servera 2008 za domen Litware.
  - D. Funkcionalni nivo šume Windows Servera 2003 i funkcionalni nivo domena Windows Servera 2003 za domen Litware.