

# V-Implementiranje servisa AD

## SADRŽAJ

**5.1** Planiranje Aktivnog direktorijuma

**5.2** Plan Domena

**5.3** Plan prostora imena domena

**5.4** Plan strukture organizacionih jedinica

**5.5** Plan strukture lokacije

**5.6** Administrativne alatke AD

**5.7** Upravljanje Aktivnim direktorijumom

**5.8** Instaliranje i konfiguracija AD

# 5.1 Planiranje Aktivnog direktorijuma

- ❖ „Aktivni Direktorijum je *baza podataka specijalne namene*, dizajnirana da podrži relativno veliki broj read/search operacija i značajno manji broj operacija promena i unosa podataka. AD je hijerarhijski uređena, proširiva i sa mogućnošću replikacije na više hostova.“
- ❖ „AD je struktura koja se kreira na Microsoft Windows Server operativnim sistemima, čija je svrha da *memoriše i obezbeđuje informacije o mreži, domenu i korisnicima*.“
- ❖ „Aktivni Direktorijum je servis kreiran od strane Microsoft -a, koji *smešta informacije o resursima na mreži tako da im autentifikovani korisnici kao i administratori mreže u svakom trenutku mogu lako pristupiti*. Korišćenjem AD moguće je manipulirati velikim brojem mrežnih resursa sa jednog mesta i obezbediti hijerarhijsku strukturu i pregled cele mreže.“

*AD se oslanja se na LDAP (Lightweight Directory Access) protokol, Kerberos bezbednosni protokol, DNS (Domain Name System) i FRS (File Replication) protokol.*

# 5.1 Planiranje Aktivnog direktorijuma

- Od **suštinskog značaja** za funkcionisanje mrežnog operativnog sistema u jednoj organizaciji je **da se dobro isplanira aktivni direktorijum**
- On sadrži sve **glavne komponente** koje su potrebne za nesmetano i pouzdano funkcionisanje mreže, svaki i mali propust u njegovoj postavci može u **mnogome da smanji funkcionalnost mreže**.
- Pre nego što počnemo da uvodimo servis Aktivnog Direktorijuma moramo **proučiti poslovnu i organizacionu strukturu organizacije**
- Usluge AD nisu ništa drugo nego **uredno razvrstavanje svih mrežnih resursa i upravljanje istim**, potrebno je da tačno znamo broj **servera, računara, korisnika, štampača, lokacija, bezbedonosnu politiku** i td
- Koristeći **fleksibilnost servisa AD** možemo **da kreiramo strukturu mreže koja će uspešno odgovoriti svim zahtevima organizacije**.
- Strukturu AD čine **četiri osnovne komponente**:
  - 1. plan domena,**
  - 2. plan prostora imena domena,**
  - 3. plan strukture organizacionih jedinica**
  - 4. plan strukture sajta.**

## 5.2 Plan domena

- Potrebno je da počnemo od fizičkog okruženja mreže, da odredimo osnovni domen, broj domena i njihovo hijerahijsko organizovanje.
- Fizičko okruženje uključuje lokacije objekata u mreži, broj korisnika na svakoj lokaciji, broj potrebnih servera kao i servisa na tim serverima, vrstu mreže, brzinu veze, broj i kvalitet WAN konekcija i td.
- Potrebno je da se razmotre i druge infrastrukture koje organizacija već koristi kao da li postoji već DNS struktura, *Microsoft Exchange* i td.
- Pre instaliranja moramo da izaberemo kakav kontroler domena želimo da instaliramo: da li je to prvi kontroler domena za novi domen ili samo želimo da dodamo nov kontroler domena u postojeći domen.
- Ako izaberemo da to bude prvi kontroler domena za novi domen, istovremeno ćemo formirati i kontroler domena i novi domen.
- Nakon toga treba odrediti da li taj novi domen pripada novoj šumi, da li je on podređen domen u postojećem stablu domena ili predstavlja jedno novo stablo domena u postojećoj šumi.
- Dodavanje novog kontrolera u već postojeći domen pravimo *ravnopravni kontroler* domena.

## 5.2 Plan domena

- Ravnopravni kontroleri domena obezbeđuju redundantnost i smanjuju opterećenje postojećih kontrolera domena.
- Kad određujemo osnovni domen moramo da vodimo računa da je on prvi domen koji pravimo u AD, pa predstavlja i najvažniji domen
- Njegova osnovna uloga je da definiše infrastrukturu cele mreže i da upravlja istom pa je dobro da on bude namenski i da isključivo služi za administriranje infrastrukture celokupne mreže (stabla ili šume) zbog:
  - ✓ kontrolisanja broja administratora koji mogu da prave izmene,
  - ✓ jednostavno je izvršiti njegovo repliciranje jer je po veličini mali,
  - ✓ retko zastareva jer je njegova jedina uloga da služi kao osnova,
  - ✓ laka prenosivost vlasništva nad domenom bez premeštanja resursa.
- Nakon određivanja osnovnog domena šume, planiranje strukture domena treba da započnemo od sledećeg podređenog domena
- Preporuka je da se doda samo taj jedan domen a da druge domene dodamo samo u slučaju kada taj domen više ne može da ispuni zahteve
- Za pravljenje više domena moraju da postoje opravdani razlozi: očuvanje postojeće strukture, admin. i fizička podeljenost, bezbednost

# 5.3 Plan prostora imena domena

- U servisu AD domeni imaju imena koja podležu DNS pravilima.
- Razlikujemo dva prostora imena i to **unutrašnji** (interni prostor imena) i **spoljašnji** (eksterni prostor imena). Dva izbora:
  - 1.unutrašnji prostor imena isti kao i spoljašnji: dobra strana je da su imena domena potpuno ista a loša strana je da zahteva mnogo složeniju strukturu konfigurisanja mreže sa *firewall/proxy* serverima.
  - 2.unutrašnji i spoljašnji prostor imena razdvojeni: nema poklapanja ili dupliranja održavanja a i konfigurisanje klijenata je jednostavnije, ali postoje dvostruka imena za prijavljivanje na domen.
- Ime treba da je **jednostavno i da asocira na stvarnu namenu domena**
- Kod davanja imena osnovnom domenu treba voditi računa da se ono **neće menjati**, jer svaka izmena tog imena **može kasnije biti nemoguća**
- Treba koristiti **standardne ASCII karaktere koji podležu DNS pravilima** (RFC 1035), a izbegavati neke specijalne karaktere koji nisu standardni
- Broj nivoa domena treba ograničiti (**preporuka tri do četiri, max. pet**).
- Domen treba da ima **jedinstveno ime unutar sebi nadređenog domena**.
- Dužina imena domena treba da bude što manja, **ne duža od 255 znaka**.

# 5.4 Plan strukture organizacionih jedinica

*OJ predstavlja skladište koje definiše strukturu unutar nekog domena.*

- One se mogu hijerahijski organizovati u vidu ugnježdavanja.
- OJ predstavljaju najmanje jedinice na kojima se može dodeliti grupna strategija ili delegirati administriranje.
- Služi za upravljanje resursima na osnovu modela organizacije, tako da administratori mogu da delegiraju administrativne zadatke svim ili samo jednoj organizacionoj jedinici
- Planiranje OJ podrazumeva da dobro znamo funkcionalnu organizaciju i strukturu preduzeća, kao i njihovim administrativnim potrebama.
- Postoji više razloga zašto se prave organizacione jedinice i to su:
  - ✓ *Lakše održavanje resursa*
  - ✓ *Lakše delegiranje administrativnih zadataka*
  - ✓ *Lakše deljenje korisnika prema grupnim strategijama*
- Broj OJ u domenu nije ograničen i zavisi od potreba organizacije
- Jedino je neophodno je da OJ prvog nivoa budu jedinstvene u domenu
- Preporučuje se da hijerahijska organizacija bude što plića

## 5.4 Plan strukture organizacionih jedinica

- Postoji nekoliko uobičajenih modela koji nam pomažu da odredimo hijerarhiju koja nam najviše odgovara i to:
- **Geografski model** – kako su geografske granice stabilne, prednost ovog modela je da administratorima znatno olakšava pronalaženje resursa na mreži. Ovaj model ne mora potpuno da odražava način poslovanja organizacije za koju se OJ pravi, ali se uz manje modifikacije može uspešno primeniti.
  - **Organizacioni model** – ovde se OJ prave upravo prema strukturi jedne organizacije, prema odelenjima i sektorima što je prihvatljivo i lako shvatljivo. On olakšava jednostavno delegiranje zadataka, dodelu prava i zabrana, jer su resursi upravo tako i razdeljeni po OJ sa istim interesima.
  - **Objektni model** – podela resursa po OJ ovde je definisana na osnovu klase tih resursa. Klase predstavljaju skup resursa sa istim osobinama kao: korisnici, računari, grupe, štampači i td. Prednost ovog modela je da olakšava administriranje resursa, jer svaka OJ ima jednoobrazne objekte, ali se zato može dobiti veliki broj organizacionih jedinica.



# 5.5 Plan strukture lokacije

*Lokacija ili sajt predstavlja deo fizičke strukture AD i predstavlja kombinaciju jedne ili više podmreža na bazi IP protokola koje su povezane vrlo brzim i pouzdanim vezama.*

- Jedan domen može da obuhvati više lokacija kao što i jedna lokacija može da obuhvati više domena ili njegovih delova.
- Glavna uloga lokacije je da obezbedi dobru povezanost na mreži.
- Način njegove realizacije utiče na proces prijavljivanja korisnika i provere njihove autentičnosti, kao i na replikaciju direktorijuma.
- Projektovanje sajta za LAN mrežu je veoma jednostavno – **brze veze**
- Treba voditi računa kod mreža koje se prostiru na nekoliko fiz.lokacija
- Ovde treba obratiti pažnju na:
  1. **fizičke karakteristike** tih lokacija,
  2. tačno definisati **fizičke lokacije** koje čine domene,
  3. odrediti **oblasti mreže** koje bi mogle da se povežu u sajtove,
  4. identifikujete **fizičke veze** koje povezuju te sajtove,
  5. obezbedite **otpornost na greške pomoću** mosta za povezivanje
  6. odrediti **način, vreme i cenu** replikacije.

# 5.6 Administrativne alatke AD

Windows Server poseduje moćne i fleksibilne alate koje nam olakšavaju administriranje jedne složene i velike baze podataka kao što je to AD:

✓ Alatke za AD iz paketa *Active Directory Administrative Center*

✓ *Active Directory* modul za *Windows PowerShell*

✓ Administrativne konzole za Aktivni Direktorijum – instaliraju se automatski na kontrolerima domena kada se instalira AD i mogu biti instalirane i na drugim serverima putem *Administrative Tools*:

- *Active Directory Domains And Trusts* - obezbeđuje interfejs za upravljanje domenima i odnosima poverenja između šuma i domena.
- *Active Directory Sites And Services* - AD se daju informacije o fizičkoj konfiguraciji mreže. Te informacije AD koristi da bi mogao da odredi kako da vrši repliciranje direktorijuma između kontrolera domena.
- *Active Directory Users And Computers* - namena je da dodamo, izmenimo, obrišemo i organizujemo korisničke i računarske naloge, bezbedonosne i distributivne grupe i prijavljene resurse u okviru našeg domena, da upravljamo i kontrolerima domena kao i OJ.
- *Active Directory Schema*-služi za izmenu atributa AD i klasa objekata u šemi AD. Retko se koristi za izmene pa se podrazumevno ne instalira.

# 5.7 Upravljanje AD

## 1. Obezbeđivanje integriteta baze podataka

AD predstavlja jednu vrstu transakcione baze podataka pa je potrebno voditi dnevnik transakcija koji omogućava poništavanje operacija po segmentima i sigurno završavanje transakcija u bazi.

## 2. Pravljenje rezervnih kopija servisa Aktivnog Direktorijuma

Podaci koji se čuvaju u AD predstavljaju jako bitne podatke za efikasno funkcionisanje jedne mreže pa je potrebno praviti rezervne kopije AD.

## 3. Premeštanje Aktivnog Direktorijuma

Ovu aktivnost vršimo u slučaju da se fizički disk, na kome se nalazi baza podataka, ošteti ili on jednostavno otkaže. Da bi to uradili služimo se programom *ntdsutil.exe* koja radi u režimu *Directory Service Restore*.

## 4. Defragmentacija baze podataka

Postoje dva načina defragmentacije baze podataka i to **automatska** (na vezi) i **ručna** (van veze). Automatsko defragmentisanje svoje baze podataka, AD obavlja svakih **12 sati** potpuno samostalno i to radi u sklopu svog procesa uklanjanja smeća (*Garbage Collection*).

# 5.7 Integriranje AD sa drugim servisima

**1. AD i SQL Server** – Mehanizam baze podataka AD zove se *Jet*, koju koristi i Microsoftov Access. Međutim, AD može sasvim lepo da koristi i SQL Server kao svoj mehanizam baze podataka. Tako da ako nam trebaju i kontrola pristupa i dobre performanse, koje samo SQL Server može da nam pruži, preporučuje se da zajedno koriste i AD i SQL Server.

**2. AD i Microsoft Exchange** – Microsoft Exchange omogućuje nam da u okviru mreže pouzdano razmenjujemo gotovo sve podatke. Posebna pogodnost je ta da se on može vrlo lako integrisati sa AD i da on u njemu podrazumevano skladišti sve podatke o korisnicima i njihovim nalogima.

**3. AD i DNS** – DNS je osnovni način pronalaženja usluga i servera AD u domenu. Klijenti i različiti servisi koriste DNS za pronalaženje osnovnog domena radi prijavljivanja i administriranja mreže. Pravilo je da barem jedan DNS mora biti instaliran u šumi domena da bi AD ispravno radio.

**4. Nadgledanje povereničkih odnosa i replikovanje** – *Active Directory Replication Monitor (Replmon.exe)* predstavlja grafički alat za nadgledanje operacija niskog nivoa i performansi replikovanja osnovnog domena – upravljača u kompletnom domenu.

# 5.8 Instaliranje Aktivnog direktorijuma

1. Izabrati **Server Manager** iz menija (*task bar*).
2. Iz **Server Manager** Dashboard izabrati **Add roles and features**.

Server Manager

Server Manager > Dashboard

Manage Tools View Help

Dashboard

- Local Server
- All Servers
- File and Storage Services >

WELCOME TO SERVER MANAGER

1 Configure this local server

- 2 [Add roles and features](#)
- 3 Add other servers to manage
- 4 Create a server group

QUICK START

WHAT'S NEW

LEARN MORE

Hide

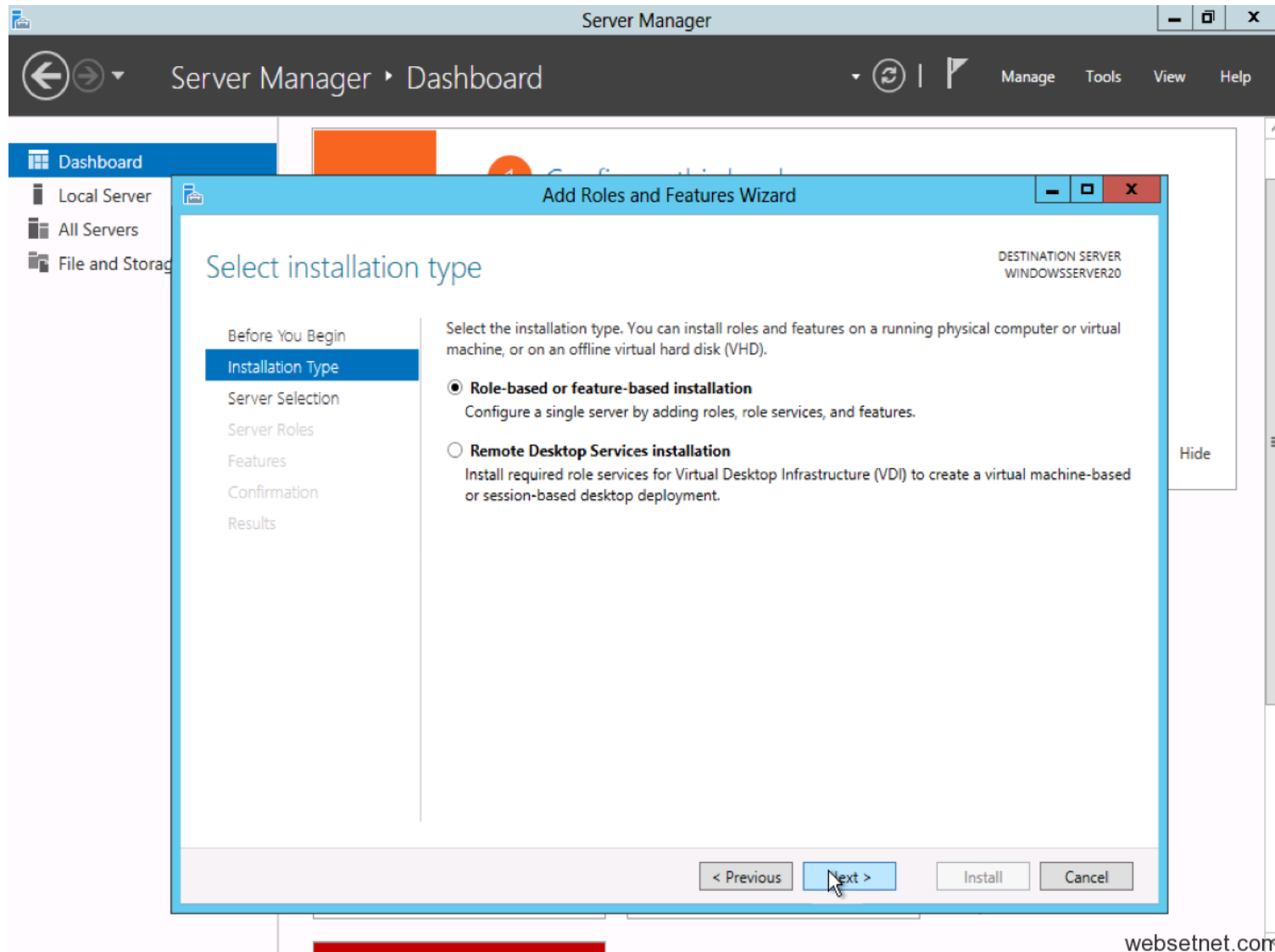
ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

File and Storage Services 1	Local Server 1
Manageability	Manageability
Events	Events
Performance	Services
BPA results	Performance
	BPA results

# 5.8 Instaliranje Aktivnog direktorijuma

3. Selektovati **Role-based or features-based** instalaciju iz ekrana **Installation Type** screen i nakon toga potvrditi sa opcijom **Next**.



# 5.8 Instaliranje Aktivnog direktorijuma

4. Tekući server je označen po *default*.

Potvrditi izbor sa **Next** da bi došli do **Server Roles** tab.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. In the top right corner, it says 'DESTINATION SERVER WINDOWSSERVER20'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted in blue), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the following text: 'Select a server or a virtual hard disk on which to install roles and features.' Below this are two radio buttons: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Underneath is a 'Server Pool' section with a 'Filter:' text box. Below the filter is a table with the following data:

Name	IP Address	Operating System
WINDOWSSERVER20	10.181.15.198,...	Microsoft Windows Server 2012 Standard

Below the table, it says '1 Computer(s) found'. A paragraph of text follows: 'This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the bottom of the window, there are four buttons: '< Previous', 'Next >' (with a mouse cursor over it), 'Install', and 'Cancel'. The website 'websetnet.com' is visible in the bottom right corner.

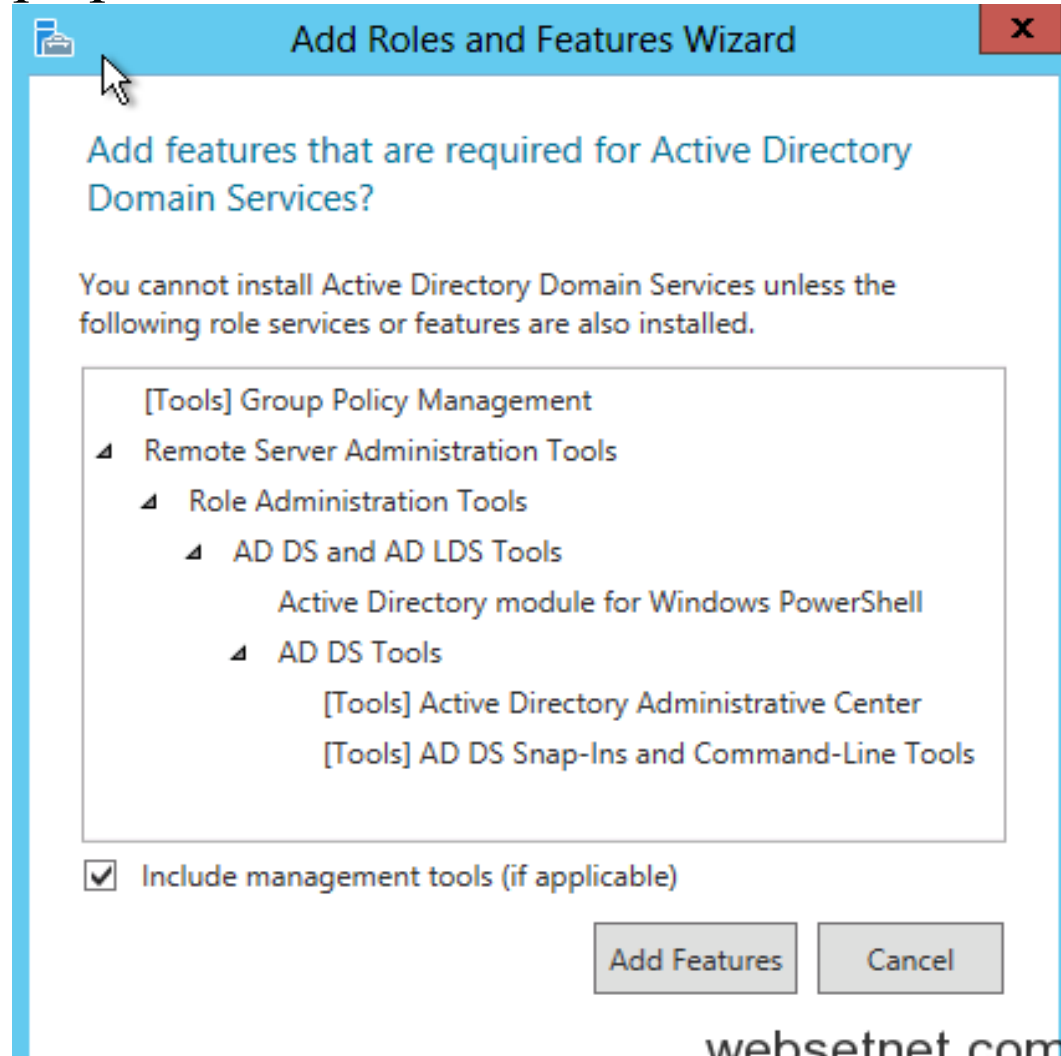
# 5.8 Instaliranje Aktivnog direktorijuma

5. Sa strane Server Roles označite marker u kvadratiču do **Active Directory Domain Services**. Pojaviće se dodatne role, servisi i mogućnosti koje će se instalirati pa pritisnite **Add Features**.

## Napomena:

*Postoje i druge opcije kao Certificate services, federation services, lightweight directory services i rights management.*

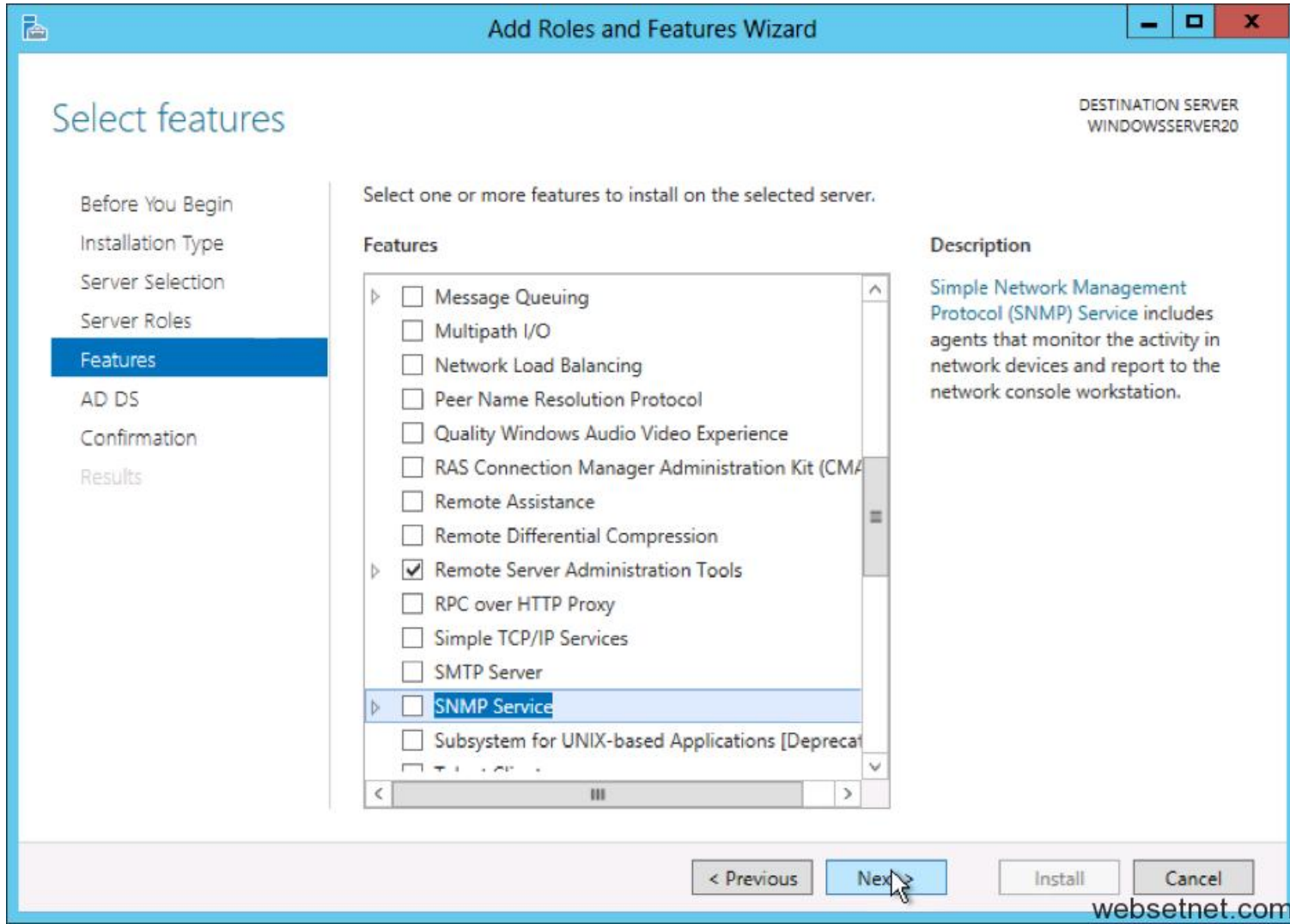
*Međutim usluge Domain Services su osnovne i one moraju prvo da se instaliraju pre nego bilo koji drugi servisi.*





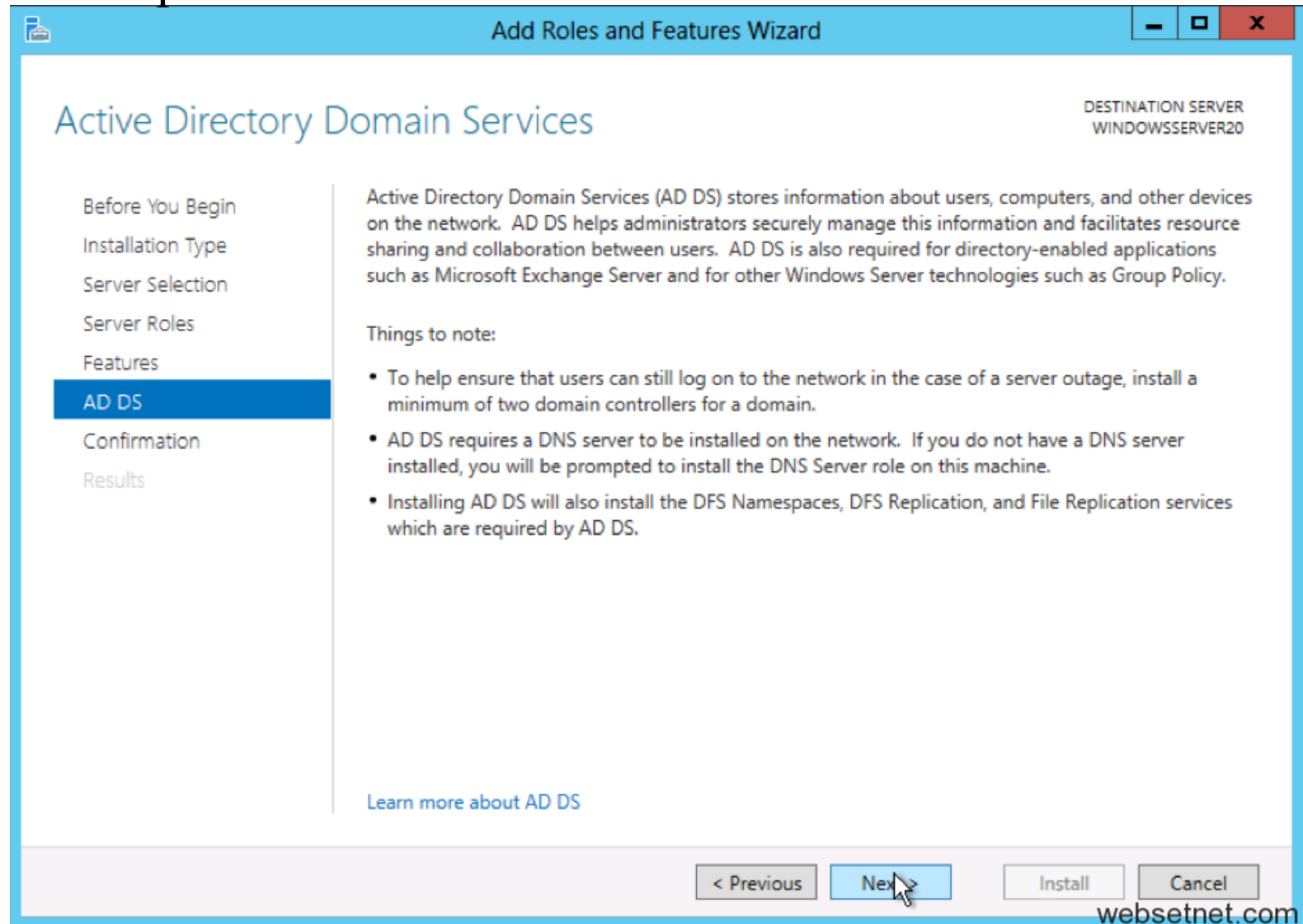
# 5.8 Instaliranje Aktivnog direktorijuma

6. Pogledajte i izaberite opcione funkcije za instalaciju tokom instalacije AD DS postavljanjem markera (čekirajte) u polje pored bilo koje željene karakteristike. Kada završite kliknite na **Next**.



# 5.8 Instaliranje Aktivnog direktorijuma

7. Izaberite **AD DS** i još jednom pregledajte sve opcije koje ste označili i ako se slažete pritisnite izbor **Next**

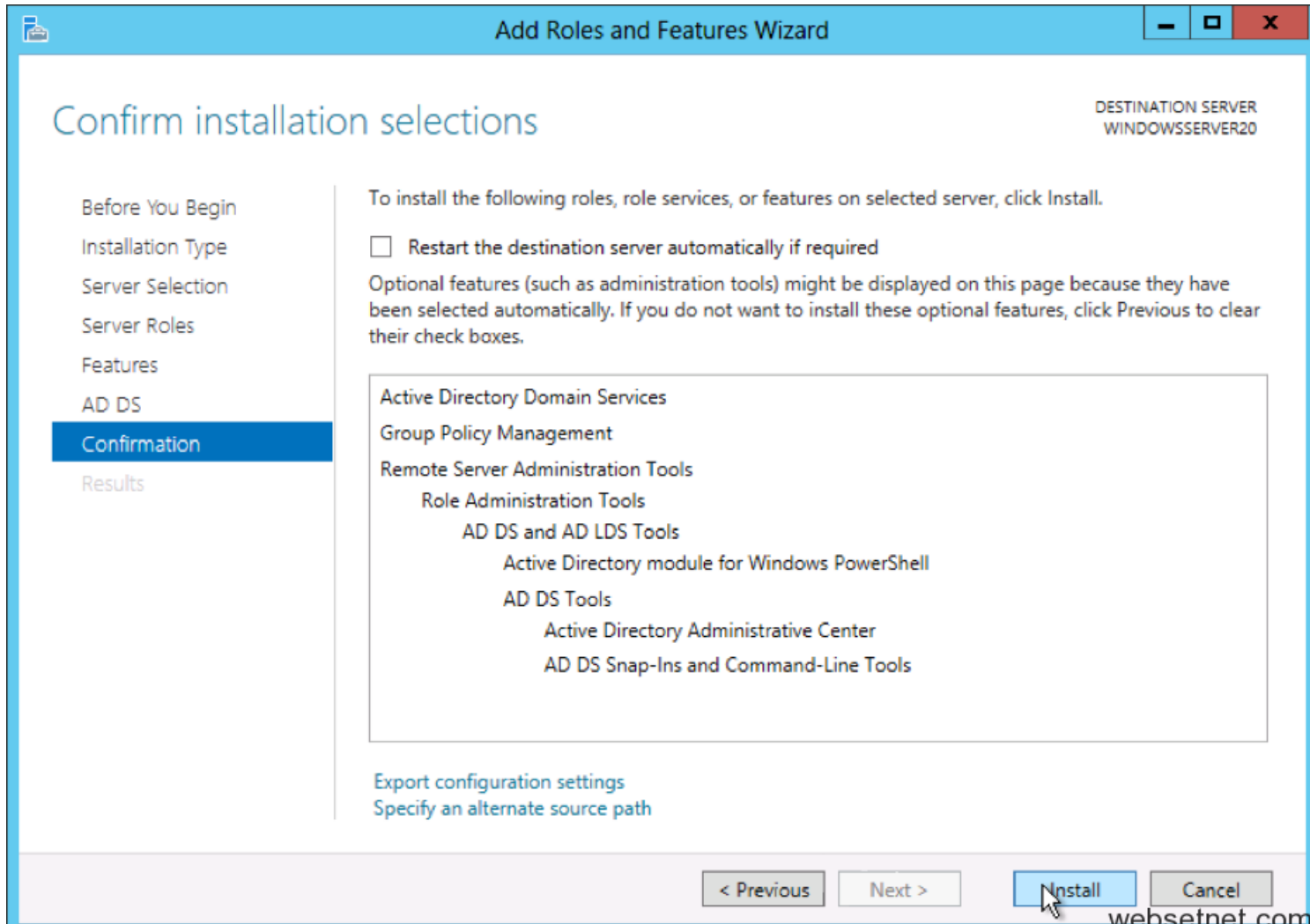


# 5.8 Instaliranje Aktivnog direktorijuma

8. Pregledajte postavke instalacije i kliknite na **Install**.

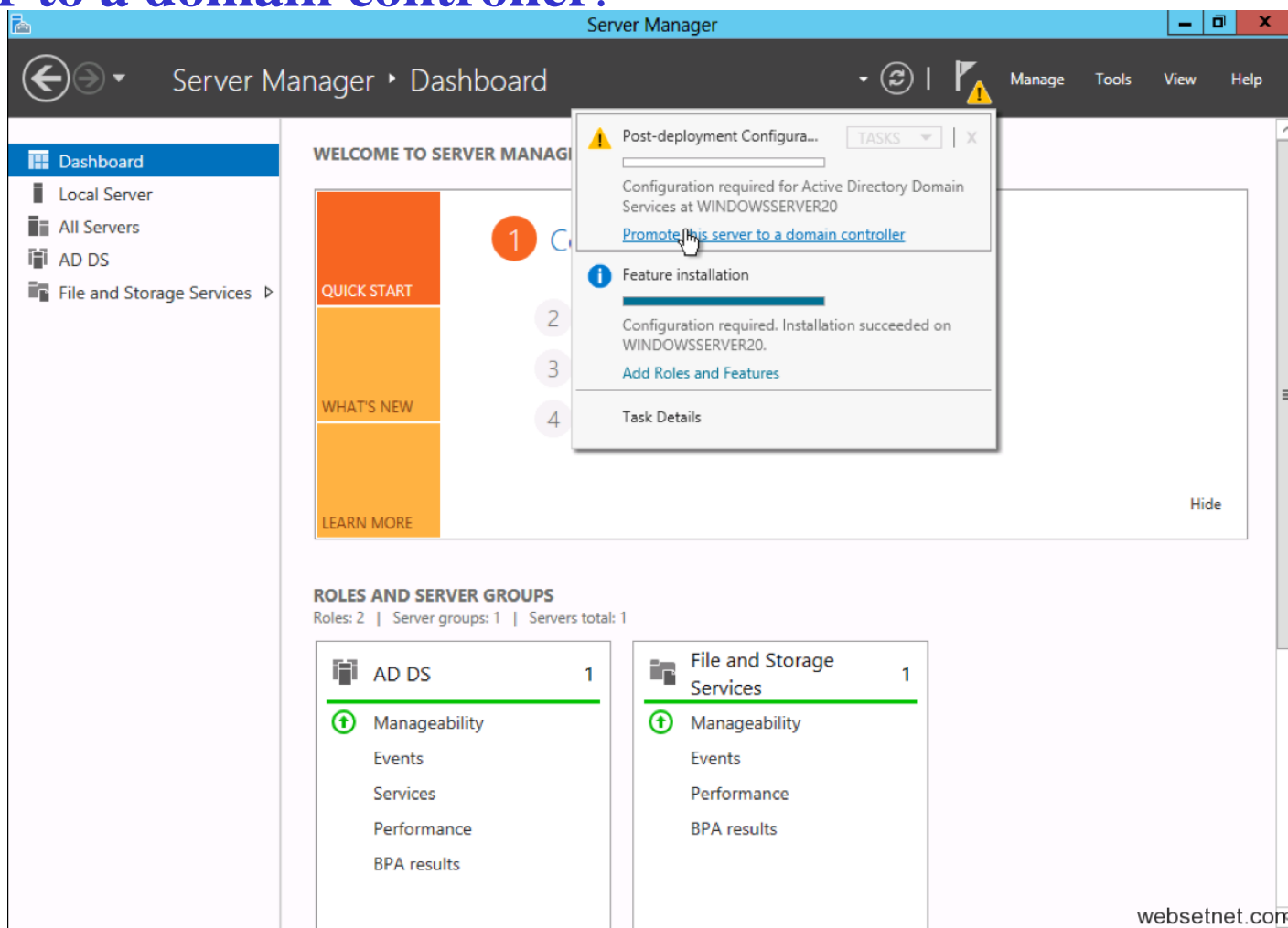
Napomena: kako instalacija napreduje biće prikazano na ekranu.

*Jednom instalirana AD DS rola biće prikazana na “Server Manager”*



# 5.8 Konfigurisanje Aktivnog direktorijuma

1. Otvorite program **Server Manager** iz menija (*task bar*).
2. Izaberite **Notifications Pane** selektovanjem ikone **Notifications** sa vrha Server Manager. Iz prozora notifikacije izaberite opciju **Promote this server to a domain controller**.



The screenshot displays the Windows Server Manager dashboard. A notification window is open, titled "Post-deployment Configura...", with a yellow warning icon. The notification text reads: "Configuration required for Active Directory Domain Services at WINDOWSSERVER20" and includes a blue link: "Promote this server to a domain controller". Below the notification, a "Feature installation" section shows a progress bar and the text: "Configuration required. Installation succeeded on WINDOWSSERVER20." with a link "Add Roles and Features". The notification also includes a "Task Details" section. In the background, the Server Manager dashboard is visible, showing a "QUICK START" section with a red circle containing the number "1" next to the "Promote this server to a domain controller" link. The dashboard also shows "ROLES AND SERVER GROUPS" with two columns: "AD DS" and "File and Storage Services", each with a count of "1".

Server Manager

Server Manager ▶ Dashboard

Manage Tools View Help

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 2 | Server groups: 1 | Servers total: 1

AD DS 1

File and Storage Services 1

Manageability

Events

Services

Performance

BPA results

Manageability

Events

Performance

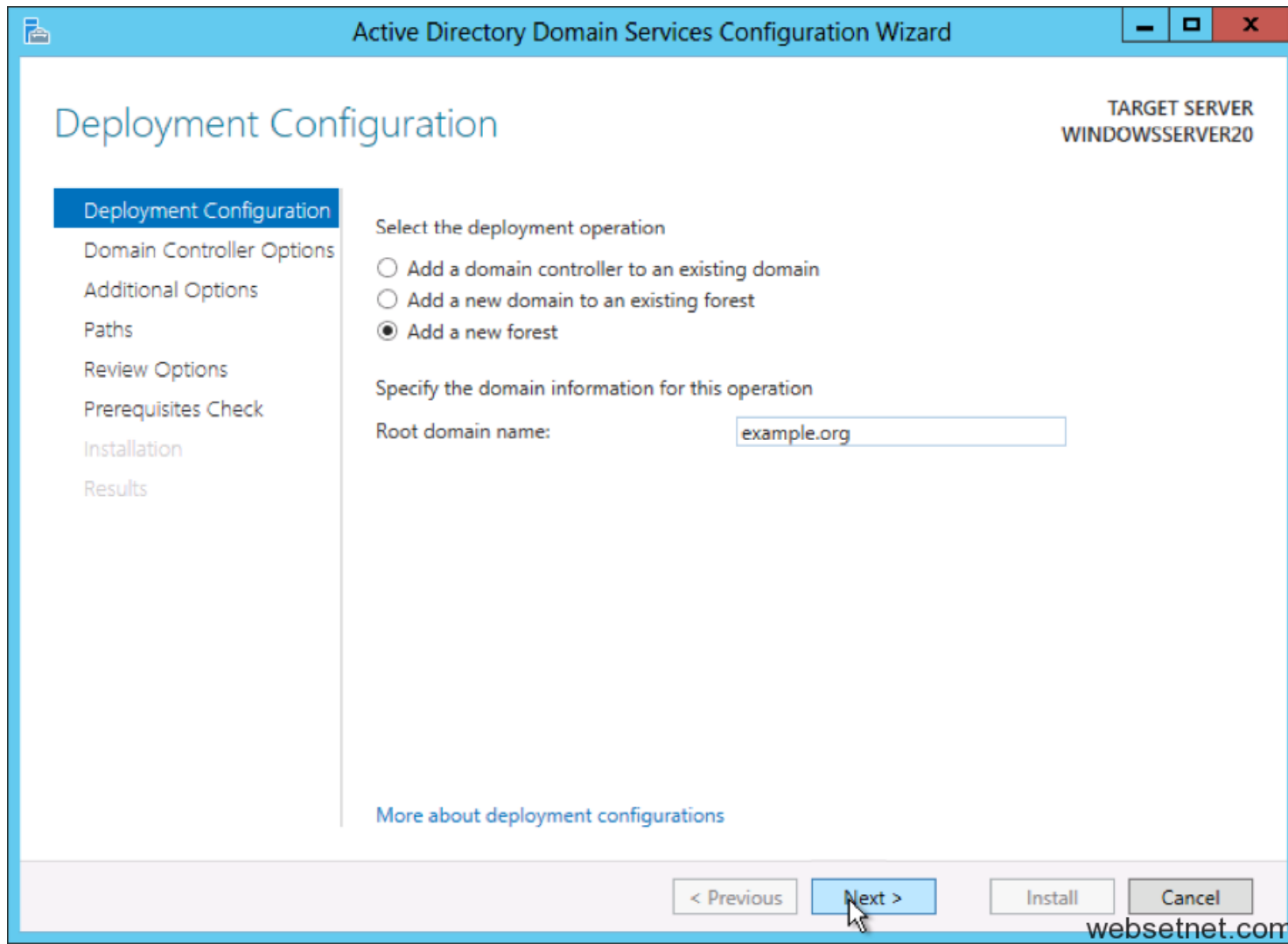
BPA results

Hide

websetnet.com

# 5.8 Konfigurisanje Aktivnog direktorijuma

3. Iz menija **Deployment Configuration** izaberite **Add a new forest** iz menija (radio dugmad) sa desne strane. Unesite vaše *root domain* ime u polje **Root domain name**.



The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes a folder icon, the text 'Active Directory Domain Services Configuration Wizard', and standard window controls (minimize, maximize, close). The main window has a light blue header with 'Deployment Configuration' on the left and 'TARGET SERVER WINDOWSSERVER20' on the right. A left-hand navigation pane lists several steps: 'Deployment Configuration' (highlighted in blue), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select the deployment operation' and contains three radio button options: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). Below this, the text 'Specify the domain information for this operation' is followed by a label 'Root domain name:' and a text input field containing 'example.org'. At the bottom of the window, there are four buttons: '< Previous', 'Next >' (with a mouse cursor over it), 'Install', and 'Cancel'. A link 'More about deployment configurations' is located at the bottom left of the main content area. The website 'websetnet.com' is visible in the bottom right corner of the image.

# 5.8 Konfigurisanje Aktivnog direktorijuma

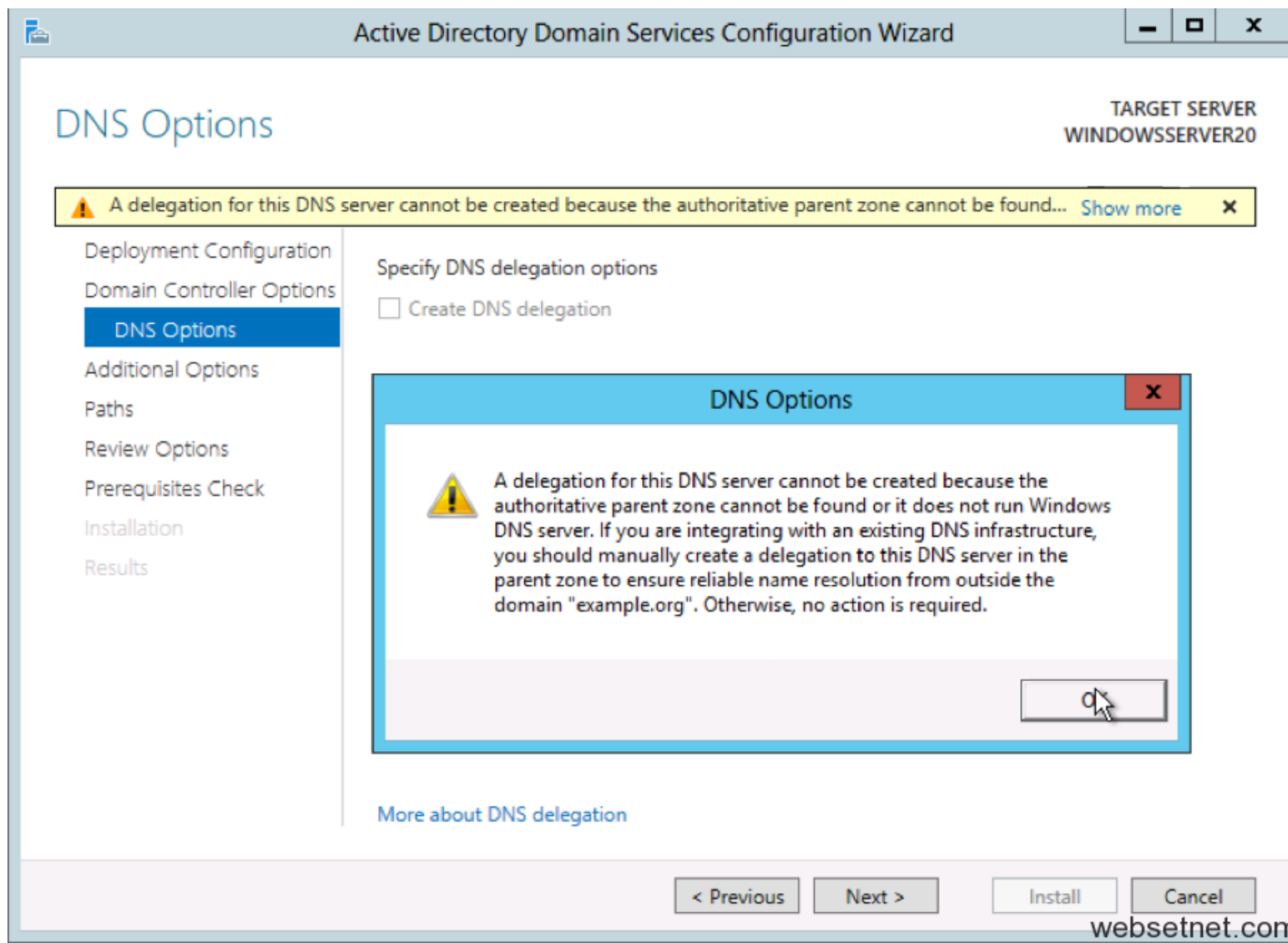
4. Pregledati i izabrati **Domain and Forest** funkcionalne nivoe. Unesite **DSRM password** u odgovarajuće polje za lozinku koji će vam trebati u slučaju podizanja Domain Controller u *recovery* modu rada.

Napomena : *Izbor koji ovde uradite imaće trajne efekte na funkcijama kao i mogućnostima servera kontrolora domena. Za više informacija o Domain/Forest funkcionalnosti pogledajte zvaničnu dokumentaciju Microsoft-a*

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar indicates the target server is 'WINDOWSSERVER20'. The main heading is 'Domain Controller Options'. On the left, a navigation pane lists steps: Deployment Configuration, Domain Controller Options (highlighted), DNS Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main area is divided into sections: 'Select functional level of the new forest and root domain' with dropdowns for 'Forest functional level' and 'Domain functional level', both set to 'Windows Server 2012'; 'Specify domain controller capabilities' with checkboxes for 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked); and 'Type the Directory Services Restore Mode (DSRM) password' with two password input fields. At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A watermark 'websetnet.com' is visible in the bottom right corner.

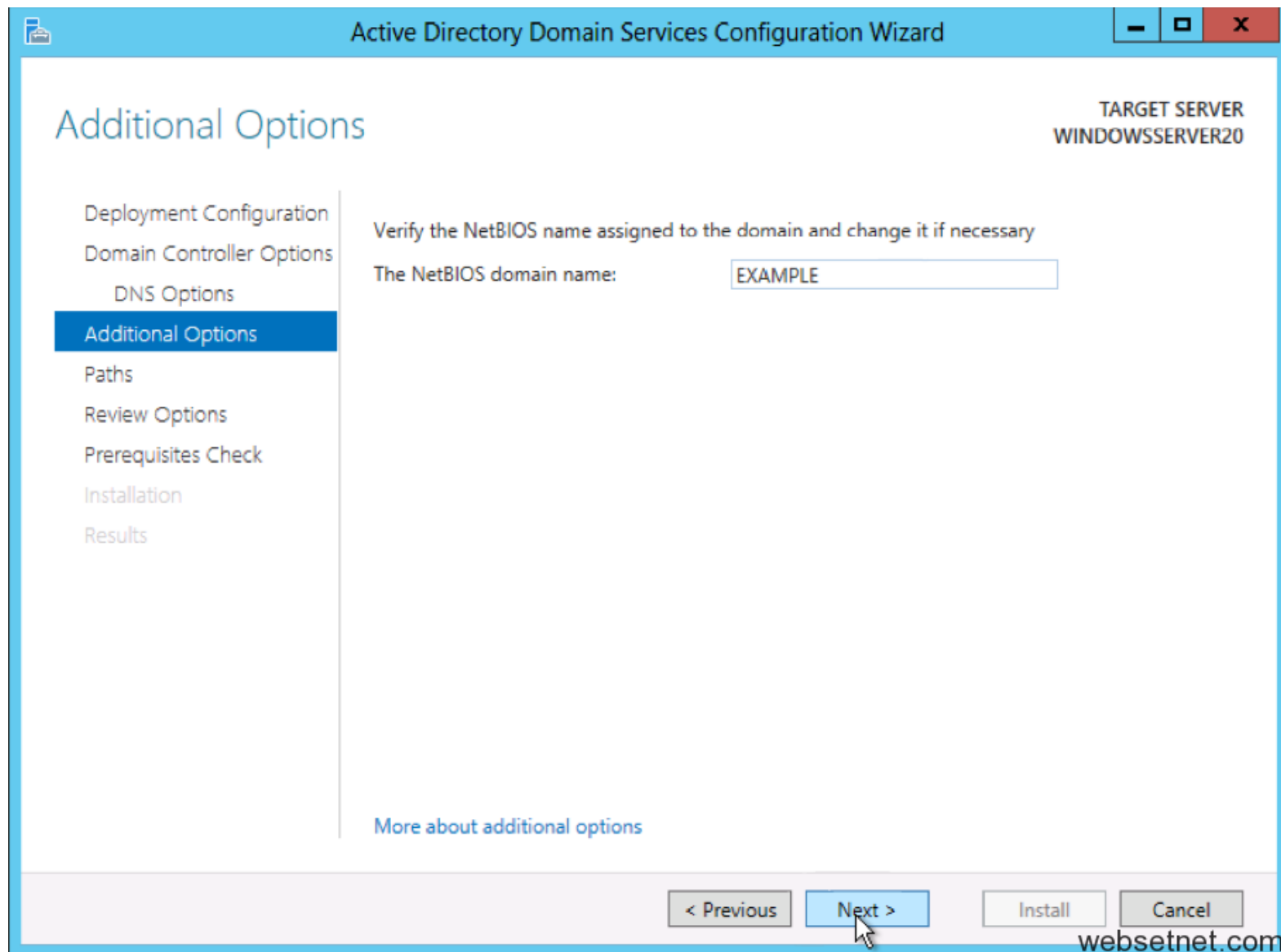
# 5.8 Konfigurisanje Aktivnog direktorijuma

5. Pogledajte upozorenja koja ste dobili u prozoru *DNS Options* i nakon toga pritisnite izbor **Next**



# 5.8 Konfigurisanje Aktivnog direktorijuma

6. Potvrdite ili unesite **NetBIOS** ime i zatim pritisnite **Next**.





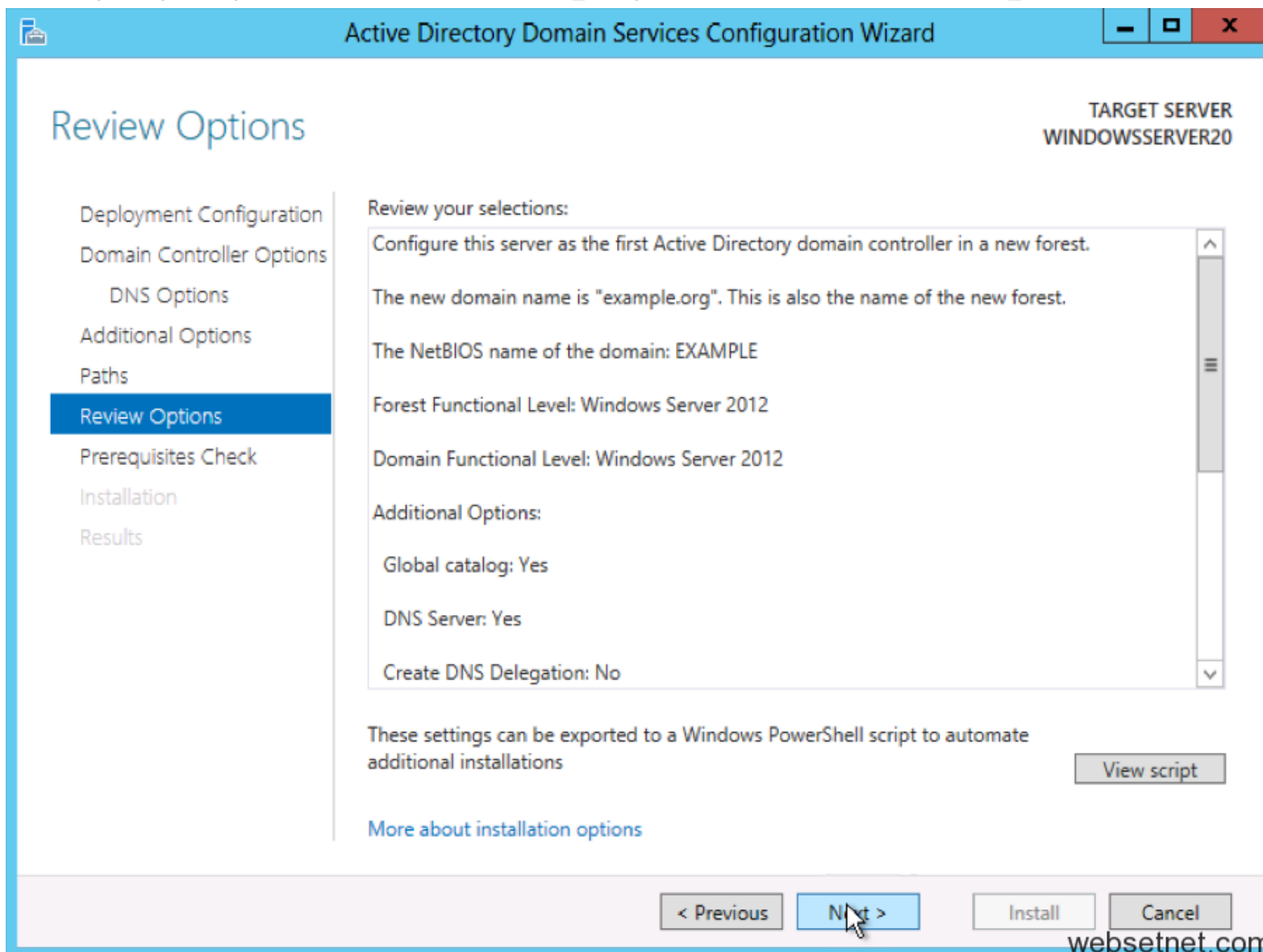
# 5.8 Konfigurisanje Aktivnog direktorijuma

7. Unesite lokacije za **SYSVOL**, **Log** fajlove, i **Database** i zatim pritisnite **Next**

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the text 'Active Directory Domain Services Configuration Wizard' and standard window control buttons. The main window area is titled 'Paths' and indicates the 'TARGET SERVER' as 'WINDOWSSERVER20'. On the left, a navigation pane lists the following steps: 'Deployment Configuration', 'Domain Controller Options', 'DNS Options', 'Additional Options', 'Paths' (which is highlighted in blue), 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area contains the instruction 'Specify the location of the AD DS database, log files, and SYSVOL'. Below this, there are three input fields with browse buttons (three dots): 'Database folder:' with the value 'C:\Windows\NTDS', 'Log files folder:' with the value 'C:\Windows\NTDS', and 'SYSVOL folder:' with the value 'C:\Windows\SYSVOL'. At the bottom of the wizard, there are four buttons: '< Previous', 'Next' (with a mouse cursor over it), 'Install', and 'Cancel'. A watermark 'websetnet.com' is visible in the bottom right corner.

# 5.8 Konfigurisanje Aktivnog direktorijuma

8. Pregledajte još jednom zadate opcije i ako se slažete pritisnite **Next**.



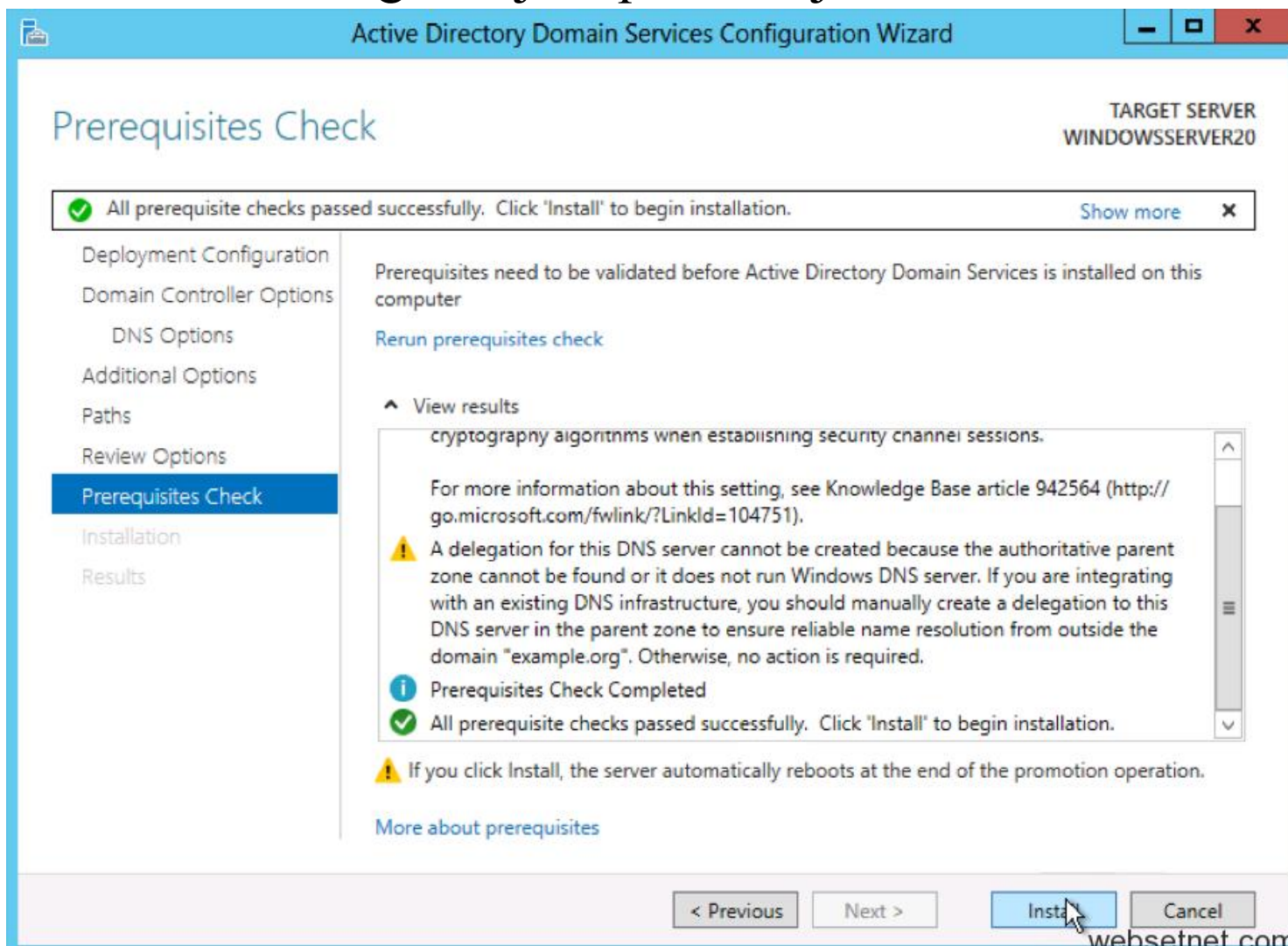
# 5.8 Konfigurisanje Aktivnog direktorijuma

9. e samostalno proveriti da li su obezbeđeni svi neophodni preduslovi tj. da li su oni instalirani na sistemu i ako je to uredu dozvoliće da se nastaviti sa konfiguracijom pritiskanjem na **Install**.

Napomena :

e

*automatski biti ponovo pokrenut nakon završetka kompletne instalacije.*



Hvala na pažnji !!!



Pitanja

? ? ?