

Windows Server 2012 i Network discovery dubioze



Zbog imperativa sigurnosti i Microsoft, poput ostalih proizvođača operativnih sustava, sve pomalo mijenja defaultne postavke svojih Windowsa. Trend je takav da su windoze, posebno serverske edicije, iz verzije u verziju sve zatvorenije nakon inicijalne instalacije. Linuxašima je taj pristup dobro poznat – tijekom prve instalacije OS-a aktivira se minimalni broj servisa, tek toliko da se OS može dignuti i potom konfigurirati tj. prilagođavati za obnašanje planirane uloge. Kali distro je u tome najekstremniji – iako se defaultno instaliraju i Apache i SSH i PostgreSQL.... niti jedan servis ne otvara port, niti se OS oglašava na mreži.

Glede Kalia, postoje dobri razlozi za njegovo „konspirativno“ ponašanje (o tome čemo uskoro pisati). Vratimo se windozama. U serverskoj ediciji – jer i Windows i Linux desktop edicije nastoje biti maksimalno susretljive naspram korisnika - uvedene su, pored onih kompleksnijih, i neke u osnovi benigne promjene, ali irritantne utoliko što OS ne prihvati neke admin akcije i ne izvijesti o tome, ili pak prihvati promjenu ali izostane opomena o posljedicama. Na ovako neljubazno ponašanje OS-a uvijek užurban sistemac jednostavno nije naviknut, pa nakon par pokušaja neuspješnog rekonfiguriranja proglaši server glupim & bugovitim. Tipična sitna ali dinamitna promjena koja Windows adminu zadaje puno sekiracije je Network Discovery funkcionalnost, jer nepravilno podešena dovodi do nepouzdanosti ili čak do neupotrebljivosti preglednika Network, aplikacije kojom browsamo računala na LAN-u. Nižom sličicom ilustriramo na što ciljamo.

A screenshot of the Windows File Explorer interface. The top navigation bar shows 'File', 'Network', and 'View'. Below the toolbar are standard file operations: back, forward, up, search, and network navigation. The left sidebar has 'Favorites' (Desktop, Downloads, Recent places), 'This PC' (highlighted), and 'Network' (highlighted with a blue border). The main pane displays a table of network resources. The columns are 'Name', 'Category', 'Workgroup', and 'Network location'. The 'Computer' section lists several Windows machines: AD-CA, SQL2008T1, SQL2008T2, DC1, FSC1, FSC2, KLASTERINA, SQL-VMM, and WIN81RALE. All are categorized as 'Computer', belong to the 'AD' workgroup, and are located in 'corp.hr'. A 'Multifunction Devices (1)' section shows a Lexmark MX511de printer, which is a 'Multifunction...' device located in 'corp.hr'.

Name	Category	Workgroup	Network location
AD-CA	Computer	AD	
SQL2008T1	Computer	AD	
SQL2008T2	Computer	AD	
DC1	Computer	CORP	corp.hr
FSC1	Computer	CORP	corp.hr
FSC2	Computer	CORP	corp.hr
KLASTERINA	Computer	CORP	corp.hr
SQL-VMM	Computer	CORP	corp.hr
WIN81RALE	Computer	CORP	corp.hr
Lexmark MX511de (O...)	Multifunction...		corp.hr

Prisjetimo se, sa Network Discovery funkcijom dopuštamo ili branimo novijim edicijama Windowsa oglašavanje svog prisustva na mreži. Funkcija je kao opcija dostupna kroz Network and Sharing Centar, i to za svaki mrežni profil zasebno, vidi nižu sliku. Odmah ističemo sljedeće: ako ne uključimo

Network Discovery već samo susjednu opciju File and Print Sharing, Windows će nas kroz Network prozor doduše informirati o drugim mrežnim čvorovima, ali te će informacije biti nepotpune!

The screenshot shows the Windows Control Panel with the 'Network and Sharing Center' selected. A red box highlights the 'Advanced sharing settings' link under the title bar. Below the title bar, there are links for 'View', 'Tools', and 'Help'. The main content area is titled 'Change sharing options for different network profiles'. It says 'Windows creates a separate network profile for each network you use. You can choose specific options for each profile.' There are two tabs: 'Private' (selected) and 'Guest or Public' (with a red box around it). Under 'Private', there are sections for 'Network discovery' and 'File and printer sharing'. Under 'Network discovery', it says 'When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.' Three radio button options are shown: 'Turn on network discovery' (unchecked), 'Turn on automatic setup of network connected devices' (checked), and 'Turn off network discovery' (selected). Under 'File and printer sharing', it says 'When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.' Two radio button options are shown: 'Turn on file and printer sharing' (unchecked) and 'Turn off file and printer sharing' (selected). The 'Guest or Public' tab has a red box around it and a dropdown arrow icon.

Sad, iole iskusniji Windows admin zna da neprisustvo nekog računala u Network prozoru ne znači, kao prvo, da to računalo nije na mreži niti, kao drugo, da se ne možemo spojiti na dijeljene resurse koje to računalo nudi, tipično, mape ili pisače. Nama sistemcima na raspolaganju su ping, telnet, nbtstat, UNC pathovi, naredbe Run i Search, IP adresa ili DNS ime umjesto NetBIOS imena (itd.)... ukratko, začas detektiramo pravo stanje, spojimo se na resurs „nepostojećeg“ računala i baš nas briga što računalo nije prikazano u Network pregledniku. Niže vidimo kako se Windows admin snašao da iz poznate mu IP adrese sazna ime računala i kojoj radnoj grupi pripada - uočite da je ciljno računalo na drugom subnetu - potom se, rabeći FQDN cilja, informira o dijeljenim mapama na tom računalu.

```
C:\>nbtstat -A 192.168.10.230
```

SU-IT:

```
Node IpAddress: [192.168.4.39] Scope Id: []
```

NetBIOS Remote Machine Name Table

Name	Type	Status
AD-CA	<00>	UNIQUE
AD	<00>	GROUP
AD-CA	<20>	UNIQUE

```
MAC Address = 00-50-56-9B-00-84
```

```
C:\>net view \\ad-ca.ad.prod.hr
```

```
Shared resources at \\ad-ca.ad.prod.hr
```

```
Share name Type Used as Comment
```

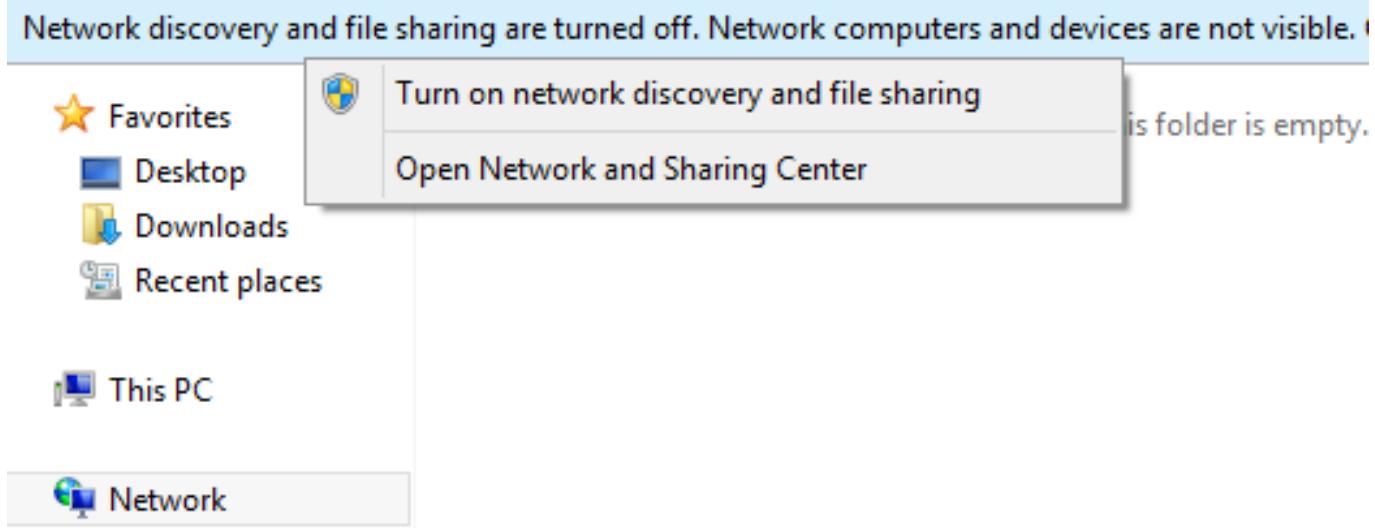
CertEnroll	Disk	Active Directory Certificate Services share
Images	Disk	
Transfer	Disk	

```
The command completed successfully.
```

Problem je što ovakve finte korisnici ne znaju. Network preglednik je njima namijenjen, kako bi kroz GUI vidjeli ciljno računalo i spojili se na njegov mrežni resurs. Budimo realni, prosječan korisnik računala tako i treba raditi tj., ako resursima na Webu pristupa Internet preglednikom, svoje svakodnevne poslove obavlja kroz „upozorene“ aplikacije, zašto bi, zaboga, drugačije radio kad treba resurse nekog računala na korporativnoj mreži?!

Stoga se Windows admini moraju, ako ne zbog sebe onda zbog svojih korisnika, upoznati sa Network Discovery funkcijom. A to upoznavanje će, kad jednom započne, potrajati nekoliko dana jer postoje razni preduvjeti koji moraju biti ispoštovani kako bi otkrivanje mreže bilo potpuno, sveobuhvatno. Važan faktor je i mrežna topologija - LAN-ovi su danas redovito isparcelizirani, tj. routerima ili layer 3 preklopnicima izdijeljeni u zasebne broadcast domene. Što za posljedicu ima, i to valja upamtiti, da će Windows računala, čak i kada su ispravno podešena za Network Discovery, u Network pregledniku prikazati samo ona računala koja su na istom subnetu, ukoliko izostane podrška infrastrukturnih servisa poput Active Directory ili WINS! Uočite ovaj „ili“ jer WINS nije potreban ako su nam sva Windows računala u domeni, konfiguirirana kako spada, a servis Computer Browser na Domain Controllerima je startan i u Automatic režimu rada.

Da bismo problematikom ovladali uz najmanje truda, dobro je opisati što treba učiniti na Windows 7/8 „da vide i budu viđena“ na lokalnoj mreži. Kad instaliramo, recimo, Windows osmicu, postavimo joj kao aktivan mrežni profil Private (ako je slučajno aktivan Public) te, napisljeku, kliknemo na Network pregledniku, OS nas izvješće da su Network Discovery i File & Printer Sharing isključeni te nudi dvije opcije, baš kao na nižoj slici.



Dakle, odaberemo li Turn on network discovery and file sharing, kroz Network preglednik uskoro ćemo vidjeti računala Windows mreže, i biti viđeni. Mogli smo isti rezultat postići i bez prijelaza u Private profil ali to je, sigurnosno gledano, promašaj jer ne želimo da nam se na lokalnom vatrozidu, u profilu Public, namijenjenom radu na nesigurnoj mreži, otvore portovi za dijeljenje datoteka i pisača.

Na nižoj slici je pravilno stanje na lokalnom vatrozidu glede Network Discovery za računalo uključeno u Windows domenu. Vjerovatno ćemo još željeti omogućiti i File and Printer Sharing u Private profilu vatrozida.

Allowed apps and features:

Name	Domain	Private	Public
<input checked="" type="checkbox"/> Core Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Distributed Transaction Coordinator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> File and Printer Sharing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> File and Printer Sharing over SMBDirect	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Netlogon Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Network Discovery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Performance Logs and Alerts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Remote Desktop	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Remote Event Log Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Kako stoje stvari sa Windows Server 2012? Idemo opet „školski“: instaliramo server, smjestimo ga u Private mrežni profil... i kad u Windows Exploreru kliknemo na Network, dobit ćemo isto upozorenje i ponudu da uključimo Network Discovery, baš kako je gore opisano za desktop windoze. Ako i sada odaberemo opciju Turn on network discovery and file sharing, serverčić će to bez pogovora prihvati. Ali to je smicalica! Network Discovery funkcionalnost nije uključena, u što se lako uvjerimo kroz Advanced sharing settings. Dodatno je zbušujuće što se u prozoru Network pojavljuju računala... naizgled je sve ok, no popis je u stvari necjelovit. Također, taj server je i dalje skriven od ostalih računala, ne prikazuje se u njihovom Network pregledniku, što važi čak i ako je server u domeni i u istom subnetu na kojem su njegovi klijenti.

U čemu je „kvaka“? Izradio sam nižu tablicu, u njoj su servisi koji utječu na stanje Network preglednika. Kad pogledamo inicijalne postavke tih servisa za serverske i desktop windoze, nadomak smo rješenja: ako želimo da nam Windows server vidi druga računala i prateće mrežne uređaje poput pisača baš onako kako ih vidi desktop edicija windoza, postavit ćemo serverske servise u isto

stanje u kojem su oni na desktop ediciji, te nakon toga još uključiti Network Discovery. To je to. Microsoft je u stvari namjerno, zbog zaštite servera, određene servise u startu onemogućio. Ali je usput zapazio adminima nelogičnim ponašanjem servera utoliko što sam ponudi aktiviranje određenih funkcionalnosti a onda to ne učini niti ne izvijesti o realnom stanju.

Vodite računa da se Computer Browser neće podići ako je isključen File and Printer Sharing jer o njemu ovisi. Uočavate, treba znati ne samo što učiniti nego i kojim redom.

/*-->*/

servis	Win 2012x	Win 8x
Comp Browser	disabled	manual
DHCP i DNS klijenti	automatic	automatic
Function Discovery*	manual	manual
Homegroup provider	/	manual
Link-Layer Tolopogy Discovery Mapper	manual	manual
Network List Service	manual	manual
Network Location Awareness	automatic	automatic
Networki Store Interface Service	automatic	automatic
SSDP Discovery	disabled	manual
UPnP Device Host	disabled	manual

Svakako treba naglasiti da browsanje Windows mreže ne ovisi samo o gore navedenim servisima. Ako netko, recimo, na WINS kartici TCP/IP protokola, disableira NetBIOS, Network preglednik tog računala postaje neupotrebljiv. Nadalje, isključivanje TCP/IP v6 protokola „zato jer ionako rabimo IPv4 parametre“ ujedno otežava prikupljanje informacija o stanju na mreži jer o tom protokolu ovisi Link-Local Multicast Name Resolution (LLMNR) protokol. U mukama će se naći i oni koji na mrežnoj kartici nemaju uključene stavke koje su uključene na nižoj slici jer sve one – osim QoS Packet Scheduler - direktno utječu na vidljivost računala na lokalnoj mreži.

Networking

This connection uses the following items:

- Client for Microsoft Networks
- File and Printer Sharing for Microsoft Networks
- QoS Packet Scheduler
- Microsoft Network Adapter Multiplexor Protocol
- Link-Layer Topology Discovery Mapper I/O Driver
- Link-Layer Topology Discovery Responder
- Internet Protocol Version 6 (TCP/IPv6)
- Internet Protocol Version 4 (TCP/IPv4)

Također, ako imamo Network Discovery u Private profilu, a učlanimo računalo u domenu, Network Discovery se neće sam uključiti u domenskom profilu. Preciznije, neće ako admin domene nije izradio grupnu politiku (GPO) za tu namjenu. Ovo je, znači, hint za admine IT pogona koji svoje windoze imaju u Windows domeni – iskoristite GPO za upravljanje funkcionalnostima što ih ovdje obrađujemo. Dobitak je dvostruk: postajete maksimalno efikasni i onemogućavate lokalnom adminu računala proizvoljne izmjene postavki jer će ih obezvrijediti GPO.

Naposljetku, tijekom nadmudrivanja s Windows računalom koje se skriva od Network preglednika, ili netočno prikazuje stanje na mreži, treba se sjetiti i lokalnog firewalla. Uzalud smo pouključivali sve servise i protokole ako je njihova interakcija sa vanjskim svijetom onemogućena vatrozidom.

Allowed apps and features:

Name	Private	Public
<input checked="" type="checkbox"/> File and Printer Sharing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Games	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> HomeGroup	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> iSCSI Service	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> JuniperNetworks.JunosPulseVpn	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Key Management Service	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Media Center Extenders	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Music	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Netlogon Service	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Network Discovery	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Kako vidimo, da bismo osposobili Network preglednik za nesmetanu uporabu, zaista moramo na dosta toga obratiti pozornost, shvatiti brojne međuzavisnosti. To je, nažalost, pravilo koje svi korisnici računala, bez obzira na zvanje & zanimanje, moraju prihvatići: što je računalo zaštićenje, teže ga je rabiti.

ned, 2014-08-24 12:27 - Ratko Žižek **Kuharice:** [Windows](#) [1]

Kategorije: [Operacijski sustavi](#) [2]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/1425>

Links

- [1] <https://sysportal.carnet.hr/taxonomy/term/18>
- [2] <https://sysportal.carnet.hr/taxonomy/term/26>