SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

Mérési utasítás **DNS**

Milyen új funkciókat nyújt ez a kiszolgálói szerepkör?

A Windows Server 2008 rendszer DNS-kiszolgáló szolgáltatása a Microsoft® Windows NT® Server, Windows 2000 Server, és Windows Server® 2003 operációs rendszerek DNS-kiszolgáló szolgáltatásaihoz képest számos új és továbbfejlesztett funkciót tartalmaz. A következő szakaszok ezeket a funkciókat mutatják be.

Zóna betöltése a háttérben

Nagy szervezeteknél, ahol az Active Directory tartományi szolgáltatásokban a DNS-adatokat tároló zónák különösen nagyok, a DNS-kiszolgáló újraindítása több, mint egy óráig is eltarthat, amíg a rendszer a DNS-adatokat beolvassa a címtárszolgáltatásokból. Ennek hatására az Active Directory tartományi szolgáltatásokon alapuló zónák betöltésének időtartama alatt a DNS-kiszolgáló gyakorlatilag elérhetetlen az ügyfelek kérései számára.

A Windows Server 2008 rendszerű DNS-kiszolgáló újraindítás közben a háttérben tölti be a zónaadatokat az Active Directory tartományi szolgáltatásokból, ezért válaszolni tud más zónák adatkérelmeire. A DNS-kiszolgáló indításkor:

- Számba veszi az összes betöltendő zónát.
- Betölti a gyökérmutatókat a fájlokból vagy az Active Directory tartományi szolgáltatások tárolójából.
- Betölti az Active Directory tartományi szolgáltatások helyett fájlban tárolt zónákat.
- Válaszol a lekérdezésekre és a távoli eljáráshívásokra (RPC).
- Legalább egy szálat létrehoz az Active Directory tartományi szolgáltatásokban tárolt zónák betöltéséhez.

Mivel a zónák betöltését több különböző szál hajtja végre, a DNS-kiszolgáló a zónák betöltése közben válaszolni tud a lekérdezésekre. Ha egy DNS-ügyfél egy már betöltött zónában található állomás adataira vonatkozó kérelmet küld el, a DNS-kiszolgáló a kívánt módon, az adat visszaküldésével válaszol (vagy az adat hiányára vonatkozó választ küld vissza). Ha a kérés egy olyan csomópontra vonatkozik, amely még nincsen betöltve a memóriába, a DNS-kiszolgáló beolvassa a csomópont adatait az Active Directory tartományi szolgáltatásokból, és megfelelően frissíti a csomópont rekordlistáját.

Miért fontos ez a funkció?

Ha a DNS-kiszolgáló a zónák betöltését a háttérben végzi, újraindításkor szinte azonnal megkezdheti a lekérdezésekre adott válaszok visszaküldését, nem kell megvárnia, hogy az összes zóna teljesen betöltődjön. A DNS-kiszolgáló válaszolni tud a már betöltött, vagy az Active Directory tartományi szolgáltatásokból beolvasható csomópontokra vonatkozó lekérdezésekre. Ez a funkció további előnyöket is biztosít, ha a zónaadatokat nem fájlban, hanem az Active Directory tartományi szolgáltatásokban tárolja: Lekérdezés fogadásakor az Active Directory tartományi szolgáltatások azonnal és aszinkron módon érhetők el, míg a fájlban tárolt zónaadatok csak a fájl szekvenciális olvasásával hozzáférhetők.

IPv6-címek támogatása

Az IP protokoll 6-os verziója (IPv6) 128 bit hosszúságú címeket határoz meg, míg az IPv4 32 bit hosszúságúakat. Ez a nagyobb mérték sokkal nagyobb számú globálisan egyedi cím létrehozását teszi lehetővé, amely fontos az internet robbanásszerű elterjedéséhez való alkalmazkodásban.

A Windows Server 2008 rendszert futtató DNS-kiszolgálók az IPv4-címekhez hasonlóan az IPv6-címeket is támogatják. A DNS beépülő modulban például az IP-címek IPv4 vagy IPv6 címformátumban is beírhatók és megjeleníthetők. A **dnscmd** parancssori eszköz is elfogadja mindkét címformátumot. Ezen felül a DNS-kiszolgáló rekurzív lekérdezéseket küldhet a csak IPv6 típusú kiszolgálóknak, és a kiszolgáló továbbítói listája IPv4 és IPv6 típusú címeket is tartalmazhat. A DHCP-ügyfelek IPv4-címek mellett (vagy helyett) IPv6-címeket is regisztrálhatnak. Végül a DNS-kiszolgáló támogatja az ip6.arpa tartománynévteret a névkereséshez.

Miért fontos ez a funkció?

Az internet világszintű elterjedésével az IPv6 címzési protokoll egyre fontosabb tényezővé válik. Az IPv6 címzés támogatásával a Windows Server 2008 biztosítja, hogy a DNS-kiszolgálók képesek legyenek azokat a meglévő és jövőbeni DNS-ügyfeleket támogatni, amelyek ki tudják használni az IPv6-címek nyújtotta előnyöket.

Hogyan lehet felkészülni erre a változásra?

Mivel a DNS-kiszolgáló az IPv4-állomás (A) erőforrásrekordjait és az IPv6-állomás (AAAA) erőforrásrekordjait is visszaküldi válaszként, győződjön meg arról, hogy a hálózaton található DNS-ügyfélszoftver az ilyen válaszokat megfelelően tudja kezelni. A kompatibilitás biztosításához szükség lehet a régebbi DNS-ügyfélszoftver frissítésére vagy cseréjére.

Írásvédett tartományvezérlő támogatása

A Windows Server 2008 egy új típusú tartományvezérlőt vezet be, az írásvédett tartományvezérlőt. Az írásvédett tartományvezérlők gyakorlatilag a tartományvezérlők árnyékmásolatát biztosítják, amelyek nem konfigurálhatók közvetlenül, ezért kevésbé sebezhetőek a támadásokkal szemben. Írásvédett tartományvezérlő olyan helyeken telepíthető, ahol a tartományvezérlő fizikai biztonsága nem garantálható.

Az írásvédett tartományvezérlők támogatásához a Windows Server 2008 rendszert futtató DNS-kiszolgáló egy új zónatípust támogat, az elsődleges írásvédett zónát (ez telephelyzónaként is ismert). Ha egy számítógép írásvédett tartományvezérlővé válik, az replikálja a DNS által használt alkalmazási címtárpartíciókat, beleértve a tartományi, a ForestDNSZones és a DomainDNSZones partíciók teljes írásvédett másolatait is. Ez biztosítja, hogy az írásvédett tartományvezérlőn futó DNS-kiszolgáló ezen címtárpartícióiban a központi tartományvezérlőn tárolt DNS-zóna teljes írásvédett másolata megtalálható legyen. Az írásvédett tartományvezérlő rendszergazdája megtekintheti az írásvédett elsődleges zóna tartalmát, de azt csak a központi tartományvezérlőn található zóna módosításával változtathatja meg.

Miért fontos ez a funkció?

Az Active Directory tartományi szolgáltatások a DNS alapján biztosítják a névfeloldás szolgáltatást hálózati ügyfelek számára. A DNS-kiszolgáló szolgáltatás módosítása szükséges ahhoz, hogy az írásvédett tartományvezérlő támogassa az Active Directory tartományi szolgáltatásokat.

GlobalNames zóna

Ma a Microsoft számos ügyfele telepíti a WINS protokollt hálózatára. A WINS szolgáltatást gyakran használják a DNS mellett másodlagos névfeloldó protokollként. A WINS egy régebbi protokoll, amely a NetBIOS protokollt használja a TCP/IP protokollok felett (NetBT). Ennek következtében lassan elavulttá válik. Viszont egyes szervezetek továbbra is használják a WINS protokollt, mert fontosnak tartják a WINS által biztosított, egycímkés nevekkel rendelkező statikus, globális rekordokat.

Annak érdekében, hogy a szervezetek áttérhessenek csak DNS-t alkalmazó környezetre (vagy biztosíthassák a globális, egycímkés nevek előnyeit a csak DNS-t alkalmazó hálózatokban), a Windows Server 2008 rendszer DNS-kiszolgáló szolgáltatása az egycímkés nevek elhelyezésére támogat egy GlobalNames nevű zónát. Általános esetben ennek a zónának a replikációs hatóköre a teljes erdőre terjed ki, amely biztosítja, hogy a zóna egyedi, egycímkés neveket biztosítson a teljes erdő számára. Ezen felül, ha a GlobalNames zóna helyének közzétételére szolgáltatáshely (SRV) erőforrásrekordokat használ, a GlobalNames zóna támogatja az egycímkés névfeloldást olyan szervezetek számára, amelyek több erdővel rendelkeznek.

A WINS szolgáltatással ellentétben a GlobalNames zóna az egycímkés névfeloldást csak bizonyos állomásnevek, általában központilag (informatikusok által) felügyelt vállalati kiszolgálók vagy webhelyek számára biztosítja. A GlobalNames zóna nem társközi egycímkés névfeloldáshoz készült (például névfeloldáshoz munkaállomások számára), és nem támogatja a dinamikus frissítéseket. A GlobalNames zónát leggyakrabban CNAME erőforrásrekordok elhelyezésére használják, amelyek az egycímkés nevek teljesen minősített tartománynevekre (FQDN) történő leképzését végzik. A WINS protokollt használó hálózatokban a GlobalNames zóna általában olyan informatikusok által felügyelt nevek számára tartalmaz erőforrásrekordokat, amelyek a WINS szolgáltatásban már statikusan konfigurálva vannak.

A GlobalNames zóna központi telepítése után az ügyfelek általi egycímkés névfeloldás a következőképpen működik:

1. A rendszer az ügyfél elsődleges DNS-utótagját hozzáfűzi az egycímkés névhez, és a lekérdezést elküldi a DNS-kiszolgálónak.
2. Ha a teljes minősített tartománynév nem oldható fel, az ügyfél a DNS-utótagok (például a Csoportházirendben megadott) keresési listájából kéri a feloldást, ha ez a lista létezik.
3. Ha egyik név sem oldható fel, az ügyfél az egycímkés név feloldását kéri.
4. Ha az egycímkés név megjelenik a GlobalNames zónában, a zónát tároló DNS-kiszolgáló feloldja a nevet. Ellenkező esetben a lekérdezés a WINS technológia használatára vált át.

A fenti egycímkés nevek engedélyezéséhez nincs szükség az ügyfélszoftver módosítására.

A GlobalNames zóna csak abban az esetben biztosítja az egycímkés névfeloldást, ha minden mérvadó DNS-kiszolgáló a Windows Server 2008 rendszert futtatja. Más DNS-kiszolgálók azonban (amelyek egyik zónának sem mérvadó kiszolgálói) futtathatnak más operációs rendszereket. Természetesen csak a GlobalNames zóna lehet az egyetlen ilyen nevű zóna az erdőben.

A legjobb teljesítmény és legjobb méretezhetőség biztosításához ajánlott a GlobalNames zónát az Active Directory tartományi szolgáltatásokkal integrálni, és minden mérvadó DNS-kiszolgálót a GlobalNames zóna helyi másolatával konfigurálni. A GlobalNames zóna több erdőbe történő központi telepítésének támogatásához a GlobalNames zóna és az Active Directory tartományi szolgáltatások integrációja szükséges.

Globális lekérdezési tiltólista

A legtöbb TCP/IP-hálózat támogatja a DNS dinamikus frissítési szolgáltatását, mivel a dinamikus frissítés a hálózati rendszergazdák és a felhasználók számára egyaránt kényelmes. A dinamikus frissítés segítségével a DNS-ügyfélszámítógépek regisztrálhatják és a DNS-kiszolgálóról dinamikusan frissíthetik erőforrásrekordjaikat, amikor az ügyfél hálózati címe vagy állomásneve változik. Ezáltal ritkábban kell kézi módszerrel karbantartani a zónarekordokat, főleg az olyan ügyfelek esetében, amelyeket gyakran áthelyeznek, illetve amelyek gyakran változtatják a helyüket, és a DHCP protokoll segítségével kapnak IP-címet. A kényelem ára azonban az, hogy egy jogosulatlan ügyfél bármilyen nem használt állomásnevet regisztrálhat, még olyat is, amelynek bizonyos alkalmazások esetében különös jelentősége van. Ezáltal a rosszindulatú felhasználók egy nevet „eltéríthetnek”, és a hálózati forgalom bizonyos típusait egy adott felhasználó számítógépére irányíthatják.

Két gyakran használt protokoll különösen ki van téve az ilyen jellegű eltérítésnek: a WPAD és az ISATAP protokoll. Ha egy hálózat nem használja ezeket a protokollokat, az ezek használatára konfigurált ügyfelek ki vannak téve a DNS dinamikus frissítése által lehetővé tett eltérítésnek. Az eltérítés megelőzéséhez a Windows Server 2008 DNS-kiszolgálói szerepköre globális lekérdezési tiltólistát tartalmaz, amellyel megelőzhető, hogy a rosszindulatú felhasználók a különös jelentőséggel bíró DNS-neveket eltérítsék.

Az alapértelmezett konfiguráció szerint a Windows Server 2008 DNS-kiszolgáló szolgáltatása kezeli a nevek listáját, és amikor a kiszolgáló hatáskörébe tartozó zónában az adott név feloldására vonatkozó kérelmet kap, figyelmen kívül hagyja azt. Ennek végrehajtásához a DNS-kiszolgáló szolgáltatása a kérelmet először összeveti a listával. Ha ennek során a név bal oldali része megegyezik a lista egy elemével, a DNS-kiszolgáló szolgáltatás arra vonatkozó választ küld a kérelemre, hogy az erőforrásrekord nem létezik abban az esetben is, ha az adott névhez állomás (A) vagy állomás (AAAA) típusú erőforrásrekord tartozik a zónában. Ebben az esetben ha az állomás (A) és az állomás (AAAA) típusú erőforrásrekord azért létezik a zónában, mert az állomás dinamikus frissítés használatával regisztrálta magát egy letiltott névvel, a DNS-kiszolgáló szolgáltatás nem oldja fel a nevet. A tiltólista kezdeti tartalma attól függ, hogy a WPAD vagy az ISATAP protokoll már telepítve van-e, amikor a DNS-kiszolgálói szerepkört hozzáadja a meglévő Windows Server 2008-példányhoz vagy a Windows Server korábbi verziójának DNS-kiszolgáló szolgáltatással frissített verziójához. A lista elemeit a **dnscmd** parancssori eszközzel is hozzáadhatja és eltávolíthatja, illetve kikapcsolhatja a tiltólista használatát.

A zóna összes mérvadó DNS-kiszolgálójának Windows Server 2008 rendszerrel kell működnie, és ugyanazzal a tiltólistával kell rendelkeznie annak érdekében, hogy azonos eredményt adjanak, amikor az ügyfelek a tiltólistán szereplő nevek feloldását kérik.

A DNS-ügyfél változásai

Bár a DNS-sel kapcsolatos változásoknak nincsenek egyenes következményei a DNS-kiszolgáló szerepkörre nézve, a Windows Vista® és Windows Server 2008 operációs rendszerek további szolgáltatásokkal bővítik a DNS-ügyfélszoftvert, amelyeket a következő szakaszok tárgyalnak.

LLMNR

A DNS-ügyfélszámítógépek az LLMNR (más néven szórásos DNS, multicast DNS vagy mDNS) szolgáltatással feloldhatják a neveket egy helyi hálózati szegmensen, ha a DNS-kiszolgáló nem elérhető. Ha például egy útválasztó meghibásodik, és az alhálózati kapcsolat a hálózat összes DNS-kiszolgálójával megszakad, az alhálózat LLMNR szolgáltatást támogató ügyfelei folytathatják a névfeloldást társközi alapon, ameddig a hálózati kapcsolat visszaáll.

Ezenkívül ha hálózati hiba esetén van szükség a névfeloldás biztosítására, az LLMNR szolgáltatás alkalmi, társközi (például egy repülőtér várótermében felépített) hálózatok létrehozásánál hasznos lehet.

Változások a keresési módszerekben, amelyekkel az ügyfelek megtalálják a tartományvezérlőket

Bizonyos körülmények között a mód, amellyel a DNS-ügyfelek megtalálják a tartományvezérlőket, hatással lehet a hálózat teljesítményére:

- A Windows Vista vagy a Windows Server 2008 rendszert futtató DNS-ügyfélszámítógépek Tartományvezérlő-lokátor összetevője rendszeresen megkeresi a tartományvezérlőt abban a tartományban, amelyhez tartozik. Ez a funkció segít elkerülni a teljesítményproblémákat, amelyek akkor keletkezhetnek, ha az ügyfél a hálózat meghibásodása idején keresi a tartományvezérlőt, és ezért a rendszer az ügyfelet egy távoli, lassú kapcsolaton elérhető tartományvezérlőhöz társítja. Korábban például, ha az ügyfélszámítógép hosszabb ideje le volt választva a hálózatról, a társítás addig folytatódott, amíg az ügyfél nem keresett egy új tartományvezérlőt. A tartományvezérlőhöz való társítás rendszeres megújításával az ügyfél csökkentheti annak a valószínűségét, hogy egy nem megfelelő tartományvezérlőhöz kapcsolódjon.
- A Windows Vista vagy a Windows Server 2008 rendszert futtató ügyfélszámítógép a véletlenszerű keresés helyett (programból, beállításjegyzék-beállításokkal vagy csoportházirenddel) konfigurálható a legközelebbi tartományvezérlő megkeresésére. Ez a funkció javíthatja a hálózati teljesítményt olyan hálózatokban, amelyek lassú kapcsolattal összekötött tartományokat tartalmaznak. Viszont mivel a legközelebbi tartományvezérlő megkeresése csökkentheti a hálózati teljesítményt, ez a funkció alapértelmezés szerint nem engedélyezett.

1. feladat

A kiszolgáló szerepkörinél állítsa be, hogy a kiszolgáló lásson el **DNS-kiszolgálói** feladatokat.(*Server Manager/ Add roles*)
Ehhez a következőkre lesz szükség:

- a gépünk DHCP-vel kap IP címet, Erre a DNS server role telepítésekor figyelmeztetést is kapunk,. Általában célszerű statikus IP címet beállítani, de most mi hagyjuk meg a dinamikus IP-t.
- A telepítés kezdetekor rövid összefoglalót kapunk a DNS server lehetőségeiről. A példában mi csak a DNS servert telepítjük, ActiveDirectory-val való integráció nélkül.
- A telepítés befejeztekor a varázsló minden szükséges változtatást elvégez, ami a szolgáltatás működéséhez kell. (A tűzfalon is kinyitja a megfelelő portokat, hogy a szolgáltatás elérhető legyen.)

2. feladat

Hozzunk létre új zónát, amelynek az adott gép a felelőse:

- A Server managerben a Roles pontnál a telepítés után megjelenik a rá vonatkozó menüpont. Itt válasszuk ki szerverünket, azon belül pedig a Forward Lookup Zones pontot(Címkeresési zónák). A menüpontnál adott segítségnek megfelelően válasszuk ki az **Action** menüben a **New Zone** pontot. Ezzel elindul a zóna paramétereit bekérő varázsló.
- Válasszuk ez elsődleges zónát.(*Primary zone...)*
- Adjuk meg a zóna nevét: zona[*gépszám*].opre3.tilb.sze.hu; IP-cím: 192.168.100.20+ [*gépszám*]
- hozzuk létre a felajánlott új zónafájlt.
- engedélyezze a biztonságos*(secure)* és nem biztonságos(*non secure*) frissítéseket is

Sokan nem készítik el a reverse lookup zónát, de több olyan program van, mely számít a PTR rekordok meglétére, ezért mindenképpen hasznos azt is elkészítenünk az általunk üzemeltetett zónához.

Az elkészítés teljesen hasonló az elsődleges zóna elkészítéséhez. Válasszuk ki a DNS role-nál most a **Reverse Lookup Zones** pontot, és az előzőhöz hasonlóan indítsuk el a varázslót az Action menüből kiválasztva a New Zone pontot. Az elkészítés során először ugyanazokat a kérdéseket kapjuk meg (szeretnénk-e engedélyezni a dinamikus frissítéseket stb.), melyekre adjuk ugyanazokat a válaszokat, mint az elsődleges zóna elkészítésénél. Ezek után a varázsló megkérdi, hogy IPv4 vagy IPv6 reverse lookup zónát szeretnénk-e létrehozni. Ebben a leírásban az IPv6-ra nem térünk ki, **válasszuk ki** a klasszikus, IPv4-et.

- Adjuk meg, hogy melyik hálózathoz tartozzon a reverse zóna (192.168.100..)
- Itt is kiválaszthatjuk, hogy új zónafájl jöjjön létre a felajánlott paraméterekkel.
- Az összefoglaló jóváhagyása után elkészül a reverse zóna is.

A zónáink ugyan már megvannak, de éles használatnál ennél több dolgot is be kell állítanunk. Ilyen pl. a SOA rekord tartalma, zónatranszfer engedélyezése, TTL értékek....

A címkeresési zónán jobb gomb, *Properties*:

- állítsa a sorozatszámot(*serial number*) 2011111500-ra amennyiben az első gyakorlati csoportba tartozik, a második csoportnak a sorozatszáma: 2011111550-től kezdődjön. (SOA rekord)
- A frissítési időköz: 15 perc (SOA rekord)
- a névszerverek közé vegye fel a tanári gépet. Teacherw.opre3.tilb.sze.hu; 192.168.100.15
- zónatransfer: az NS listában szereplő összes gép

3. feladat

Hozzon létre a címkeresési zónában az Önnel szembenlévő gépekre egy **új állomás**t, melynek paraméterei:

- név: feher[*gépszám*]
- IP-cím:192.168.100.20+[*gépszám*]
- kapcsoljuk be a PTR rekord generálását is.

Ha létrehozta az állomást, ping-elje is meg. (ping feher[*gépszám*])
Pingeljen meg egy másik fehér gépet is, amelyről tudja, hogy be lett állítva(=ül a gép előtt valaki...).

4. feladat

Ellenőrizze a DNS megfelelő működését a beépített teszttel:

- a DNS fában a névszerverünkön *Properties/Monitoring*
- simple és reverse zones-t egyaránt. A teszt sikeres, ha mindkét esetben Pass-t kapunk.

Ellenőrizze a DNS megfelelő működését az **nslookup** paranccsal.

- **nslookup**. Ebben az esetben az alapértelmezett névszerver adatait kapjuk vissza. Ha ez nem a mi gépünk, akkor állítsuk be a **server** feher[*gépszám*].opre3.tilb.sze.hu paranccsal
- írjuk be a szemben lévő fehér gép zónabeli nevét: feher[*gépszám*].zona[*gépszám*].opre3.tilb.sze.hu Ekkor megkapjuk a zónáért felelős szerver nevét IP címét, a gép nevét és IP címét.
- **set type=PTR** Ezzel jelezzük, hogy most névkeresést szeretnénk.(IP címhez adja meg a nevet)
- 192.168.100.20+[*gépszám*] itt az IP címhez tartozó gépnevet kell visszakapnunk.
- exit

Megjegyzés:
Amennyiben végzett a feladatokkal, úgy távolítsa a kiszolgálói szerepkörök közöl a DNS névkiszolgálói szerepkört.