READ-ONLY TARTOMÁNY-VEZÉRLŐ

RODC – READ-ONLY DOMAIN CONTROLLER

PALKÓ ÁDÁM, 2024.12.02., 12.N

TARTOMÁNYOK ÉS VEZÉRLŐK

2008-ban a Microsoft egy teljesen új tartományvezérlő típussal rukkolt elő, és valóban elmondható, hogy ténylegesen valós igények hozták létre ezt a típust.

A **csak olvasható tartományvezérlő** (RODC – Read-Only Domain Controller) egy olyan DC, amely tartalmazza a címtár egy példányát, azaz képes az összes tartományvezérlő feladat ellátására, de a címtár tartalma nem változtatható meg helyben.

Miért előnyös ez?

BIZTONSÁGOS

Mivel nincs globális AD módosítási lehetőség, olyan környezetbe is ajánlható, ahol fizikailag nem garantálható a biztonság, pl. egy védett szerverszobát nélkülöző telephelyre.

Ha esetleg aztán az adott szervert helyben megpróbálják feltörni, vagy történetesen eltulajdonítják, az igazán szenzitív, globális tartományi adatokhoz nem lehet majd hozzáférni semmilyen módon, hiszen helyben ezek alapértelmezés szerint nem tárolódnak.

SÁVSZÉLESSÉG- ÉS ERŐFORRÁS-TAKARÉKOS

Mivel egy telephelyre biztonságosan telepíthető, a hitelesítési folyamatokhoz (pl. belépés, helyi erőforrás elérés) nincs szükség a WAN hálózatra vagy az internetre, igaz, ekkor némi kompromisszumra kényszerülünk, lásd később.

ALKALMAZÁS- ÉS ÜZEMELTETÉS-BARÁT

Előfordulhat, hogy üzleti szempontból is fontos alkalmazások megkövetelik a tartományvezérlőt mintegy host gépként, vagy legalább a gyors elérését.

Az is elképzelhető, hogy ezt az alkalmazást más szerver híján az egyetlen (telephelyi) szerverünkre kell feltelepíteni.

Sőt, az is előfordulhat, hogy a speciális alkalmazást egy külső cég üzemelteti, azaz szüksége van interaktív belépésre, magas jogosultsági szinttel.

ALKALMAZÁS- ÉS ÜZEMELTETÉS-BARÁT

Ki az, aki szívesen ad tartomány rendszergazda jogot egy ilyen esetben a külső szervezetnek?

Viszont eddig - egy DC esetén - majdnem minden esetben muszáj volt, hiszen más lehetőségünk nem állt rendelkezésre.

Nos, a RODC esetén nyugodtabbak lehetünk, hiszen

1. nem lehet módosítani a címtár adott példányát helyben, és
2. tartományvezérlő mivolta ellenére van helyi Administrator csoport,

azaz lehetséges az AD-n kívüli minden mást üzemeltetni egy nem Domain Admin felhasználói fiókkal.

ÜZEMELTETÉS-MENTES

Nincs AD üzemeltetés, ergo nincs szükség magasabb szaktudású, Domain Admins jogosultsággal rendelkező szakemberre, hiszen nincs semmilyen a tartományhoz, erdőhöz kapcsolódó üzemeltetési feladat.

Folytassuk a RODC megismerését

a megoldandó technikai problémákkal…

A READ-ONLY CÍMTÁR-ADATBÁZIS ÉS A REPLIKÁCIÓ

Az ún. **„unidirectional” replikáció** következménye az a változás is, hogy az írható DC-k a replikációs folyamatban felismerik, hogy a partnerük egy Read-Only szerepkört tartalmaz, és ebben az esetben nem is kezdeményezik a „**pull**” típust, hiszen nem is jönne, nem is jöhetne semmilyen változás a RODC irányából.

Ez megint csak sávszélesség csökkentést jelent, és egyúttal a hídfő DC-ket sem terheljük annyira. Ide tartozik az is, hogy ez az új, egyoldalas replikáció nemcsak a címtárszolgáltatásoknál jelentkezik, hanem értelemszerűen az ugyanígy használható **DFS-R**-nél is (Distributed File System Replication).

A HITELESÍTÉSI ADATOK GYORSÍTÓTÁRAZÁSA

Alapértelmezés szerint a RODC - két kivételtől eltekintve - nem tartalmazza semmilyen felhasználói vagy számítógépfiók jelszavát. E két kivétel az RODC gépfiókja, illetve a speciális szerepet betöltő krbtgt fiók. Viszont arra van lehetőségünk, hogy bármely más fiók hitelesítési adatait gyorsítótárazzuk.

A RODC képes KDC-ként (Key Distribution Center) viselkedni a telephely felhasználói és gépei felé, azaz képes lesz tökéletes és érvényes Kerberos kulcsokat kiadni, melyeket aztán a fiókok teljes körűen használhatnak is a hitelesítési folyamatban – a központi DC-k nélkül is.

AZ ADMIN JOGOK SZÉTVÁLASZTÁSA

Mint ahogyan már említettem, a RODC-n szükséges és fontos is egy helyi magas szintű jogosultság biztosítása, ami nagyjából a lokális admin jogkörrel egyenlő – anélkül, hogy a címtár objektumaira bármilyen befolyása lenne az ebbe a csoportba tartozó felhasználóknak.

Egy ilyen fiók csak egy tartományi fiók lehet (célszerűen az adott telephely egy felhasználója), és ami még fontos, hogy ha egy másik helyszínen, egy hagyományos tartományvezérlőn lépne be ez a felhasználó, akkor ez ugyanúgy nem fog sikerülni neki, mint mielőtt megkapta volna ezt a lehetőséget a RODC-n, mivel csak azon az egyetlen RODC-n számít adminnak.

Egy fiók e csoportba történő belehelyezése egyébként kétféle módon történhet meg:

1. A parancssorból a „Dsmgmt” eszközzel
2. A RODC telepítése során a varázsló egyik lépéseként

READ-ONLY DNS

„Ha DC, akkor DNS szerver is”. Ezt a tételt a RODC esetén is tudjuk érvényesíteni. A RODC DNS szerver teljes értékű, pl. képes az összes a DNS által használt alkalmazáspartíciók replikálására (pl. a ForestDNSZones, DomainDNSZones) vagy a kliensek maradéktalan névfeloldási kéréseinek kiszolgálására.

De… a RODC jellegéből adódóan minden művelet nem történhet meg. Melyek ezek? Nos, ide tartozik pl. a kliensek automatikus regisztrációja a DDNS segítségével, vagy saját maga felvétele pl. egy AD integrált zónába, egy NS rekord alá.