Автор:
24.12.13 16:00 -

Что собой представляет контроллер домена, доступный только для чтения (RODC)?

В. *Что собой пред-став-ля-ет кон-трол-лер до-ме-на, до-ступ-ный толь-ко для чте-ния (RODC)?*

О. RODC -- новый режим кон-трол-ле-ра до-ме-на (DC) в Windows Server 2008. На таком DC можно со-хра-нить эк-зем-пляр базы дан-ных до-ме-на Active Directory (AD), до-ступ-ный толь-ко для чте-ния, но его функ-ци-о-наль-ность го-раз-до шире, чем у про-сто-го эк-зем-пля-ра базы дан-ных, при-год-но-го толь-ко для чте-ния. Ос-нов-ные функ-ции RODC:

- База дан-ных AD Domain Services (AD DS) толь-ко для чте-ния. При-ло-же-ния, ко-то-рым нужен до-ступ толь-ко для чте-ния базы дан-ных, могут ис-поль-зо-вать RODC; но все из-ме-не-ния необ-хо-ди-мо вы-пол-нять на DC с воз-мож-но-стью чте-ния и за-пи-си (RWDC), а затем реп-ли-ци-ро-вать на RODC.
- Од-но-сто-рон-няя ре-пли-ка-ция. Из RODC нель-зя рас-про-стра-нить лож-ные дан-ные по осталь-но-му до-ме-ну, даже если из-ме-не-ние сде-ла-но на RODC. Таким об-ра-зом сни-жа-ет-ся опас-ность атаки про-тив всей си-сте-мы и слож-ность струк-ту-ры репликации.
- Кон-фи-гу-ра-ция с на-бо-ром филь-тро-ван-ных ат-ри-бу-тов. Набор филь-тро-ван-ных ат-ри-бу-тов не реп-ли-ци-ру-ет-ся ни на один RODC в лесе. Если RODC ском-про-ме-ти-ро-ван и набор из-ме-нен, то в от-ли-чие от Windows Server 2003 DC, Server 2008 RWDC не реп-ли-ци-ру-ет зна-че-ния. Если воз-мож-но, лучше уста-но-вить функ-ци-о-наль-ный уро-вень леса Server 2008, за-пре-тив ис-поль-зо-ва-ние сер-ве-ров Server 2003 в лесе, где они могут ис-пор-тить дан-ные. Кроме того, важно от-ме-тить, что нель-зя до-бав-лять кри-ти-че-ские си-стем-ные ат-ри-бу-ты в набор филь-тро-ван-ных ат-ри-бу-тов RODC.
- Огра-ни-чен-ное кэ-ши-ро-ва-ние учет-ных дан-ных. RODC не хра-нит учет-ные дан-ные поль-зо-ва-те-ля или ком-пью-те-ра (за ис-клю-че-ни-ем учет-ной за-пи-си ком-пью-те-ра RODC). По-лу-чая за-прос про-вер-ки под-лин-но-сти, RODC пе-ре-да-ет его в RWDC. Затем RODC за-пра-ши-ва-ет копию учет-ных дан-ных, чтобы в бу-ду-щем са-мо-сто-я-тель-но об-слу-жи-вать за-прос. Если по-ли-ти-ка ре-пли-ка-ции па-ро-ля до-пус-ка-ет кэ-ши-ро-ва-ние учет-ных дан-ных, то они будут за-пи-са-ны в кэш, и RODC смо-жет об-слу-жи-вать за-про-сы на ре-ги-стра-цию (пока учет-ные дан-ные не изменятся).
- От-де-ле-ние воз-мож-но-стей ад-ми-ни-стра-то-ра. RODC может на-зна-чать

поль-зо-ва-те-лей ад-ми-ни-стра-то-ра-ми сер-ве-ра, не предо-став-ляя им прав в до-мене или на дру-гих DC.

- DNS толь-ко для чте-ния. RODC DNS не поз-во-ля-ет об-нов-лять кли-ен-тов и не ре-ги-стри-ру-ет за-пи-си ре-сур-сов имени службы.
- Двух-этап-ная уста-нов-ка RODC. Пер-вый этап уста-нов-ки вы-пол-ня-ет-ся ад-ми-ни-стра-то-ром с учет-ны-ми дан-ны-ми. Он со-зда-ет учет-ную за-пись AD DS для RODC со всей ин-фор-ма-ци-ей рас-пре-де-лен-ной базы дан-ных AD, в том числе име-нем учет-ной за-пи-си DC и ме-сто-на-хож-де-ни-ем сайта. Затем ад-ми-ни-стра-тор может ука-зать поль-зо-ва-те-лей и груп-пы, ко-то-рые могут вы-пол-нить вто-рой этап уста-нов-ки, обыч-но уда-лен-но. На вто-ром этапе AD DS уста-нав-ли-ва-ет-ся на RODC, и учет-ная за-пись AD DS при-вя-зы-ва-ет-ся к серверу.

RODC может реп-ли-ци-ро-вать дан-ные толь-ко с Windows Server 2008 RWDC, по-это-му ре-пли-ка-ция из кон-трол-ле-ров до-ме-на Windows Server 2003 и дру-гих Windows Server 2008 RODC невоз-мож-на.

источник: http://www.osp.ru/win2000/2008/02/4964052

{jcomments on}