Configuring replication to Read-Only Domain Controllers (RODCs)

RODCs are a special type of domain controller that store only a specific number of user passwords rather than the passwords for all users in the domain. This provides you with the special ability, should the RODC be somehow compromised, of needing to reset only a small number of user account passwords rather than all of the user account passwords in the domain.

Because they are designed for environments that are less secure than those where you typically would deploy a domain controller, RODCs only host a read-only copy of the Active Directory database. This means that RODCs cannot directly process updates to the Active Directory database and must instead pass updates on to a “writable” domain controller.

You are likely to deploy RODCs in locations that are less secure but which still require a local domain controller to process activities such as user sign-ons.

In the majority of cases, RODCs pull updates to the Active Directory database from writable domain controllers. In the following scenarios, RODCs perform inbound replication using a replicate-single-object (RSO) operation:

■■ The password of a user who has his account password stored on the RODC is changed.

■■ A DNS client performs a DNS record update, in which case the client is redirected by the RODC to a domain controller that hosts a writable copy of the target Active Directory Integrated DNS zone.

■■ The client name, DnsHostName, OsName, OSVersionInfo, supported encryption types, and LastLogonTimeStamp attributes are updated.

These replication scenarios are treated differently because they involve objects that are critical to security. If a user had to wait until the next designated cycle for the password update she organized through the service desk to replicate to her branch office's RODC, she'd be unable to sign on to her computer with that new password.

One of the key aspects to managing an RODC is controlling which user accounts have their passwords replicated to the server. User accounts that are added to the Allowed RODC Password Replication security group have their passwords replicated to the RODC as long as they aren't members of a group that has been configured with the Deny setting in the RODC's Password Replication Policy (PRP). By default, user accounts that are members of the following groups will not have account passwords replicated to any RODC:

■■ Account operators

■■ Administrators

■■ Backup operators

■■ Denied RODC password replication group

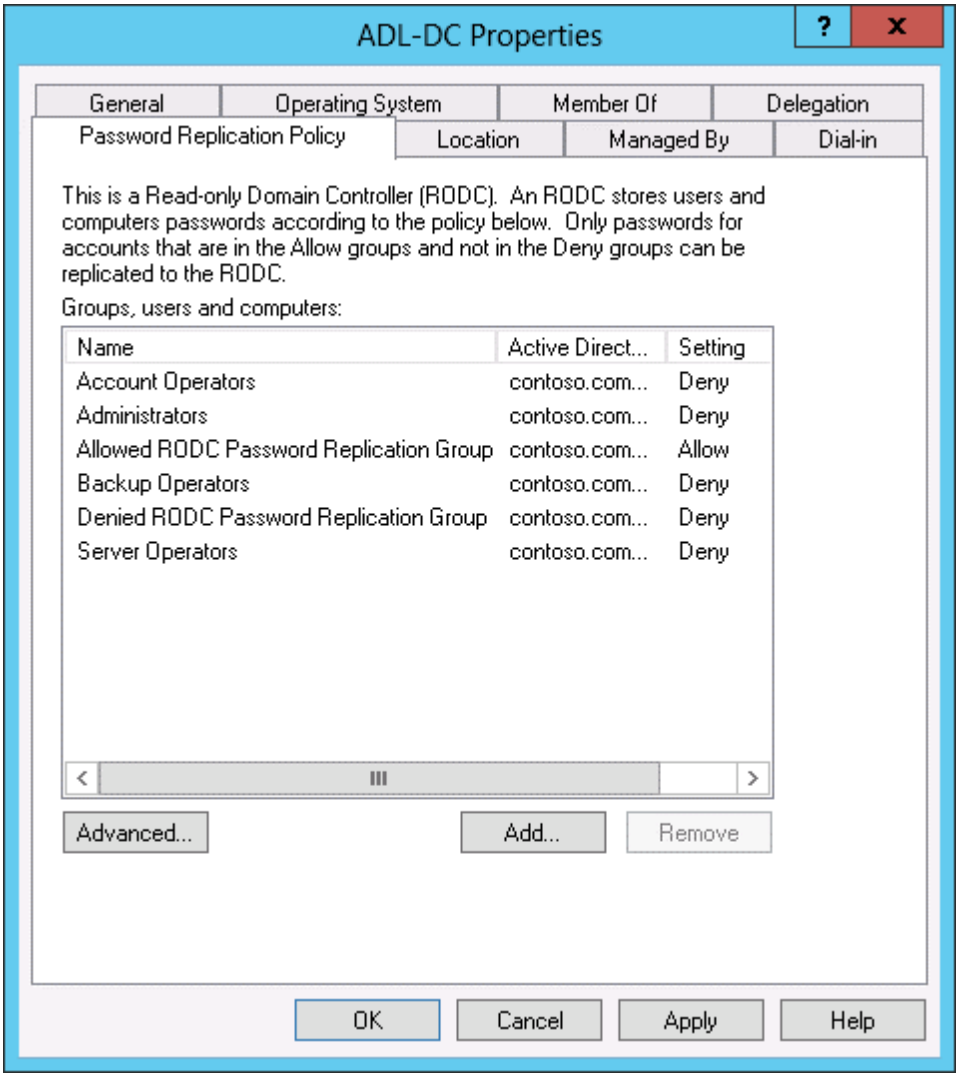
■■ Server operators

If an account password does not replicate to an RODC, it means that the person associated with that user account cannot use the RODC to authenticate. In these cases, the RODC passes the task of authenticating the user to a writable domain controller. You configure RODC password replication so that the RODC stores only the passwords of users at the site where it is deployed.

For example, you configure an RODC so that it stores only the passwords of users who work at the Melbourne site.
Users with sensitive accounts must authenticate against a writable domain controller, which you would deploy in a secure location. Because you deploy RODCs to locations where the security of the domain controller is not assured, you will naturally avoid deploying writable domain controllers in the same location. In the event that the WAN link fails, the majority of users at the site will still be able to sign on to their computers because they will authenticate using the RODC. Only users with sensitive accounts are unable to authenticate when the WAN link to a site that has RODCs fails. This is generally unproblematic because most of the time users with sensitive accounts will be located at central sites with properly secured writable domain controllers and won't be at this type of branch office site anyway.

You configure password replication policy for an RODC on the Password Replication Policy tab of the computer account's properties dialog box, as shown in Figure 5-15. Each RODC has its own password replication policy, which allows you to configure site-specific replication. For example, if you have an RODC in the Melbourne site and an RODC in the Sydney site,

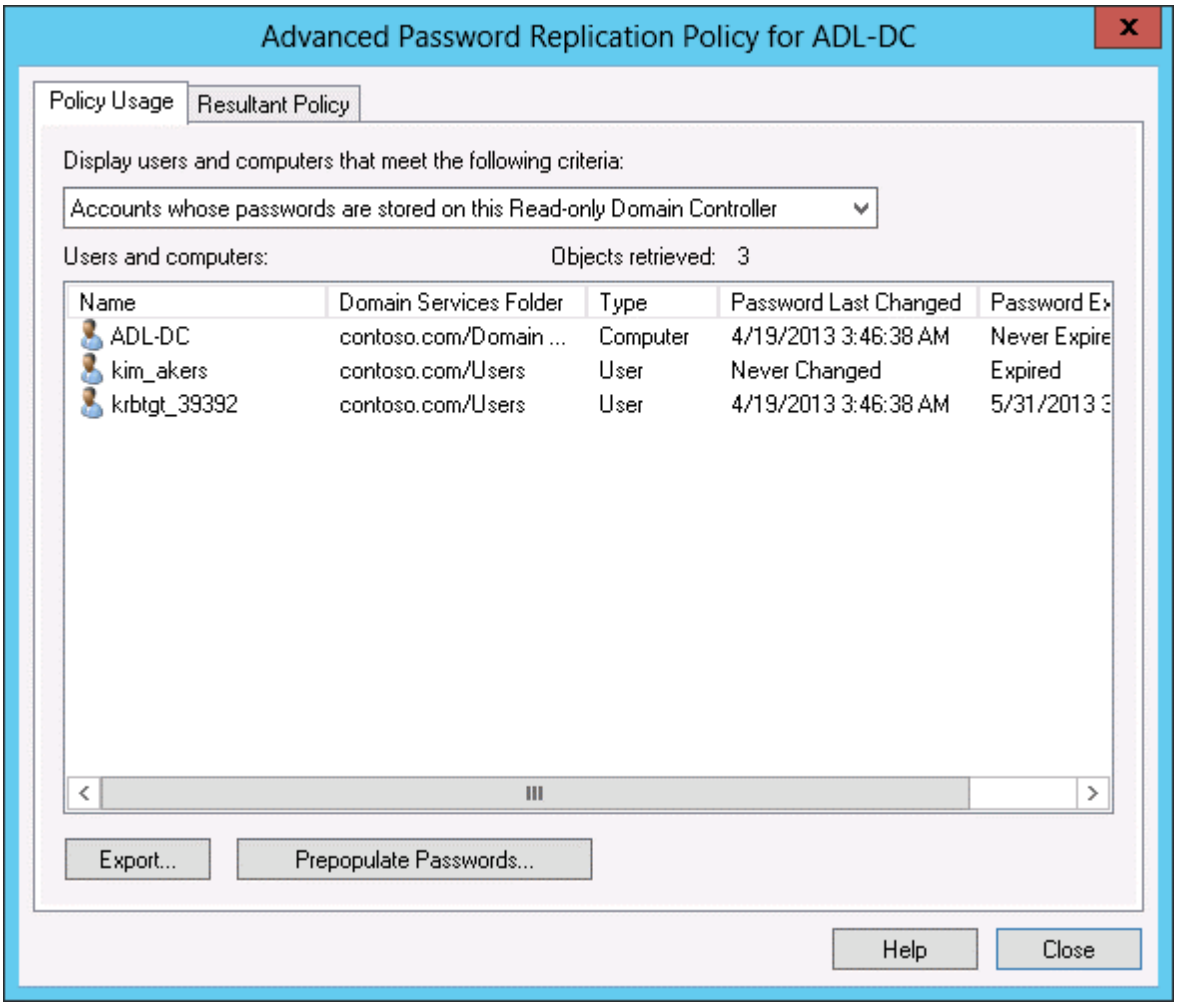
you'd configure separate password replication policies because the users who are based in the Melbourne site are going to be different from the users based in the Sydney site. The easiest way to do this is to create a security group for each site, populate it with the accounts of the users located at that site, and then add that security group to the Password Replication Policy of the RODC located at that site.



EXAM TIP

Remember which groups are blocked from having their passwords replicated to an RODC by default.

You can check which user account passwords have replicated to a specific RODC by clicking the Advanced button on the Password Replication Policy tab. This action opens the Advanced Password Replication Policy dialog box. You can also use the Prepopulate Passwords button to replicate the passwords of accounts out to the RODC. The Advanced Password Replication Policy dialog box is shown in Figure 5-16. The Resultant Policy tab of this dialog box allows you to determine if a specific user's password can be replicated to the RODC. You can use this to verify that sensitive user account passwords are not replicated to the RODC.



In the event that an RODC is compromised, such as the RODC being stolen or infected with malware that gives you reason to believe that the account database may have been compromised, you can automatically have Active Directory reset the passwords of all accounts that had replicated to the RODC by deleting the RODC computer account. When you take this step, you are prompted by the Deleting Domain Controller dialog box (shown in Figure 5-17), which presents you with the option of resetting all user account passwords and all computer account passwords. You can also export a list of reset accounts so that you can contact the users to explain why their passwords have been reset.