Realtime publishers
"Leading the Conversation"

The Essentials Series

Active Directory 2008 Operations

sponsored by
SCRIPTLOGIC

by Greg Shields

Copyright Statement

Understanding the Security Implications of Server 2008 RODCs

Technology changes. Processes change. Even business changes. But the venerable Windows domain remains. Microsoft's long-lived mechanism for consolidating authentication, security, and configuration control has seen a number of iterations in its life cycle. And yet the Windows domain has remained a near-constant within business IT environments since its inception.

What is of particular interest when one looks at the history of this network operating system (OS) is how history has a tendency to repeat itself. Servers that once were highly utilized later become underutilized as software struggled to keep up with advances in hardware. Later yet, the situation swings as virtualization consolidates low-use servers onto a single physical host. Disruptive technologies such as Terminal Services bring client/server computing back into the data center in ways much like the mainframes of yesteryear. With the release of Windows Server 2008, Microsoft presents us with a return of non-writeable domain controllers. Previously called Backup Domain Controllers (BDC), these new Windows Server 2008 constructs are now referred to as Read-Only Domain Controllers (RODCs).

History Repeats Itself

A strict comparison between a BDC and an RODC isn't complete without a look at the thought processes that have gone into their development. Windows NT BDCs were originally developed because of the need to ensure a single copy of the Active Directory (AD) database in a time before multi-master replication. In the traditional Windows NT network, the BDC housed a read-only copy of the AD database. It was intended for load balancing of incoming requests while housing an up-to-the-second backup should the Primary Domain Controller (PDC) go offline. Because the role of BDC was nothing more than a read-only version of the PDC, these capabilities were among its few benefits to the IT environment.

With the release of Windows 2000 Server and Windows Server 2003, Microsoft implemented multi-master replication to domain controller communication, which brought about the end for the BDC. Each domain controller was now an equal to every other, all containing a loosely contiguous copy of the AD database. This everything-to-everyone philosophy was a boon for large environments, as each domain controller could now both accept incoming authentication requests and make changes to the database itself.

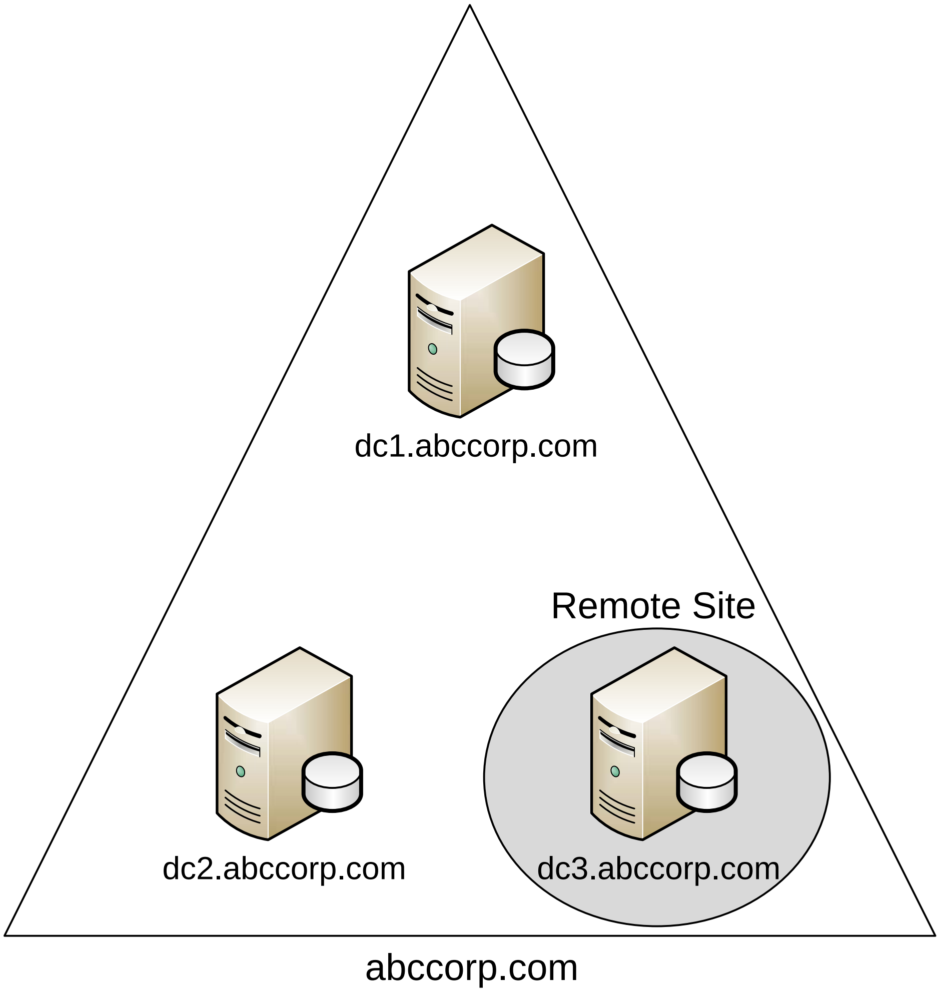


Figure 1: An AD domain with the directory database present on each domain controller.

But with these changes also came a problem. When each domain controller contains a full and complete copy of the AD database, as Figure 1 shows, the loss of even a single domain controller means the potential disclosure of an entire domain's worth of AD information. When this happens, usernames and passwords are lost, as is personnel information in situations in which AD records have been populated with HR information. With AD originally intended to be the database of record for employee information, both technical and personal, any domain controller loss would be a significant security incident for an IT organization.

The good news is that this problem isn't necessarily a high risk for all environments. In most, the physical theft of a domain controller is somewhat difficult. Data centers are typically highly secured locations, often requiring multiple mechanisms for entry. A would-be perpetrator would require substantial effort to physically enter a corporate data center and expect to get a domain controller's hard drives out the door without arousing some level of suspicion.

But not all IT environments store every domain controller in a locked-down data center. Quasi-secured locations and those with branch offices of only a few personnel are a particular concern. In a situation in which data center-grade physical security doesn't make financial sense, yet local domain controller access is needed, the result is often a domain controller that ends up under an employee's desk or stored in a closet. Although the physical removal of a domain controller from a data center is difficult, such situations bring to light a greater potential for data loss.

Introducing the RODC

Due to this problem, with Windows Server 2008, the venerable BDC makes a repeat appearance. This time, however, it arrives with new capabilities that make it a compelling fit for environments like those previously discussed. A Windows Server 2008 RODC is indeed a read-only copy of the AD database, but RODCs are different in that a Domain Administrator can choose which accounts are replicated to the RODC.

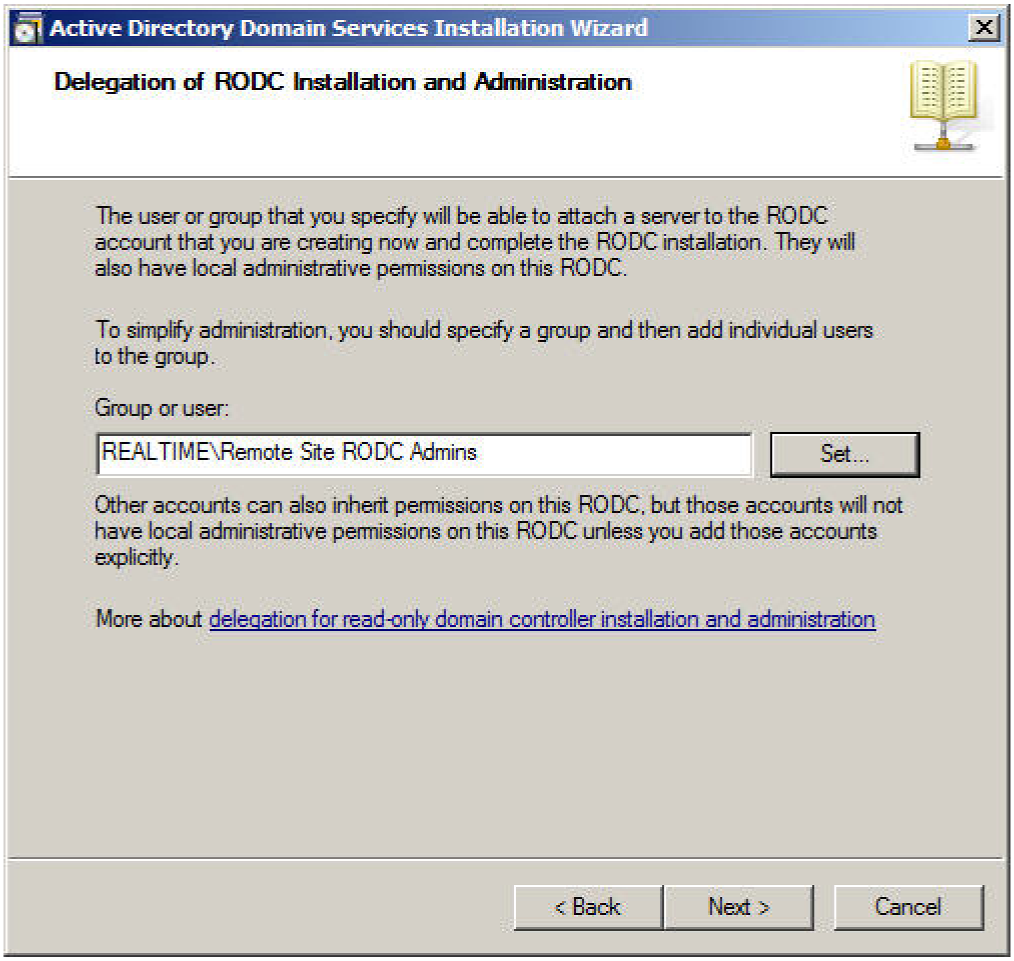
By selecting only those accounts that are local, the risk of deploying domain controllers to remote or quasi-secured locations significantly lessens. Looking back at Figure 1, if *abccorp.com* chose to deploy *dc3.abccorp.com* as an RODC, the Domain Administrator would have the added ability to replicate only the accounts appropriate to its remote site. If that domain controller is later lost, the only accounts with the potential for compromise—and therefore re-permissioning or re-creation—are those specific to the remote site.

Another problem with traditional domain controllers is their reliance on Domain Administrators for local administration. Unlike all other Windows servers, an administrator on a traditional domain controller must be a Domain Administrator. This requirement is to protect the AD database from error or compromise by a down-level administrator. But it also introduces a management headache for Domain Administrators who do not want or do not have time for the management responsibilities of the domain controller such as patching, configuration, application installation, and other administrative activities.

This headache is particularly challenging in the same remote site situations discussed earlier. In those sites, administrative responsibility for local servers is often assigned to a semi-trusted individual local to the site. This assignment allows the local person to complete patching and other operations without requiring central office IT assistance. Because of the security architecture intrinsic to domain controller alone, the only way to effectively allow this delegation to occur is to promote the part-time remote site administrator to a full Domain Administrator.

In developing the RODC, Microsoft has addressed this additional problem and created a new group designed to assist. On any deployed RODC, it is possible to grant local administrator rights to a user or group without needing to grant Domain Administrator privileges. Doing so enables far-reaching organizations to specify a local administrator with the privileges necessary to triage, troubleshoot, and otherwise administer the local RODC without needing additional Domain Administrator access. Figure 2 shows a screenshot from the DCPROMO process where this user or group can be identified.

Be aware that the read-only nature of RODCs extends to DNS as well. If DNS zones are stored within AD, updates to those zones will need to occur on a full domain controller instance. The same holds true for applications that require writing to AD as part of their daily operations, such as Microsoft Exchange. These applications also will require a full domain controller in order to complete the writing and updating processes required for their operation.



Delegation of RODC Installation and Administration

The user or group that you specify will be able to attach a server to the RODC account that you are creating now and complete the RODC installation. They will also have local administrative permissions on this RODC.

To simplify administration, you should specify a group and then add individual users to the group.

Group or user:

REALTIME\Remote Site RODC Admins

Other accounts can also inherit permissions on this RODC, but those accounts will not have local administrative permissions on this RODC unless you add those accounts explicitly.

More about delegation for read-only domain controller installation and administration

Figure 2: The DCPROMO process where you can grant local administrator rights to a user or group.

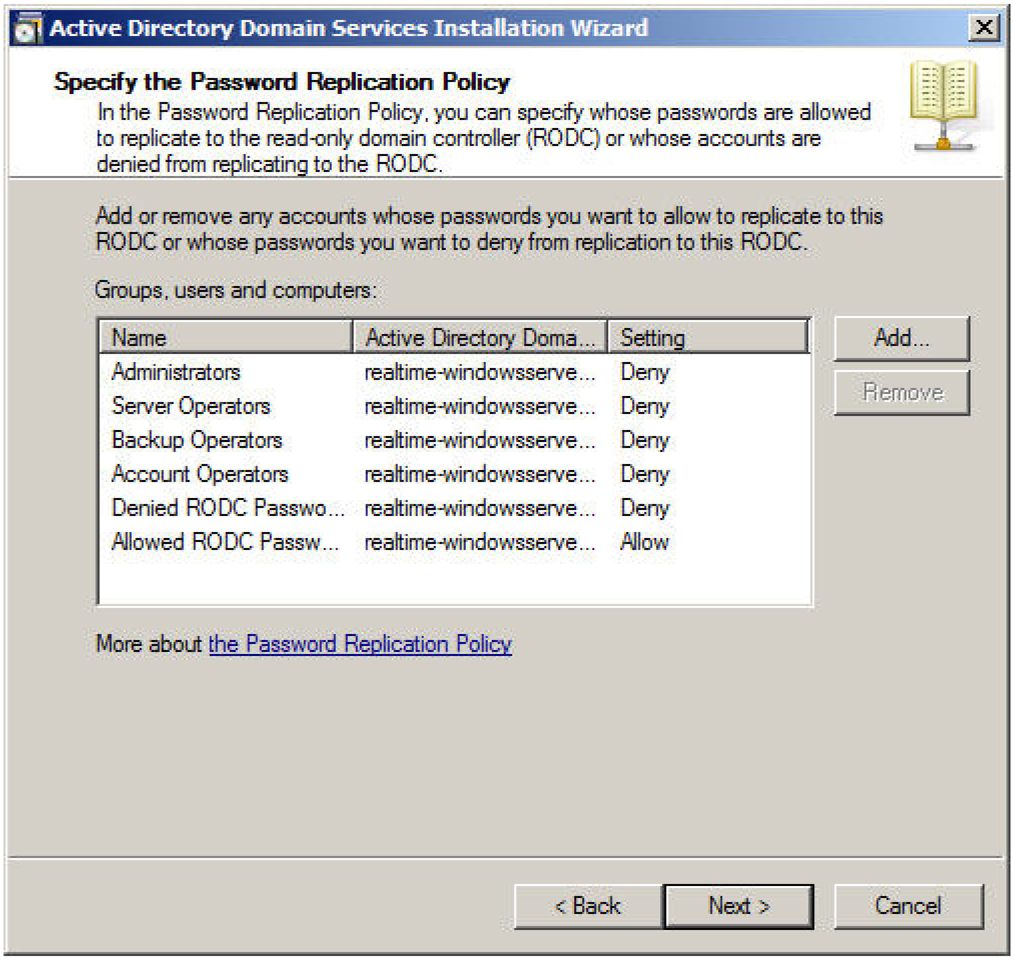
Creating an RODC

The process to create an RODC is nearly the same as the process to create a standard domain controller. Starting the process begins similarly as well. By entering *dcpromo* at the command prompt, the Active Directory Domain Services Installation Wizard starts. At the first screen, ensure that the check box is selected for *Use advanced mode installation*.

> Be aware that there are a few restrictions associated with RODCs. First, prior to the installation of any RODC, the domain schema must be modified to support their use. Do so by navigating to the *\sources\adprep* folder on Windows Server 2008 media, and from a command prompt enter *adprep.exe /rodcprep*. Once complete, allow replication to occur between the domain controllers in your domain. In addition, an RODC cannot be the first domain controller created in a domain and cannot be the first Windows Server 2008 domain controller added to an existing domain. So, prior to starting down the path for RODCs, ensure that you have a full Windows Server 2008 domain controller in place first.

Complete the installation as you would for a typical domain controller promotion, entering in the pertinent information as requested by the wizard. When the Additional Domain Controller Options window appears, ensure that the *Read-only domain controller (RODC)* check box is selected.

The next screen within the DCPROMO wizard is titled Specify the Password Replication Policy (see Figure 3). It is here that the initial decisions are made about which passwords to replicate to this particular RODC. Individual users or groups can be added to the list and set to Allow or Deny. As with NTFS configurations, the Deny attribute overrides any Allow attributes selected for users within any groups. Because of this, high-risk accounts such as Administrators, Server Operators, Backup Operators, and Account Operators are by default added to the list with the Deny attribute set. By clicking Add, it is possible to add users or groups to the list.



Active Directory Domain Services Installation Wizard

Specify the Password Replication Policy

In the Password Replication Policy, you can specify whose passwords are allowed to replicate to the read-only domain controller (RODC) or whose accounts are denied from replicating to the RODC.

Add or remove any accounts whose passwords you want to allow to replicate to this RODC or whose passwords you want to deny from replication to this RODC.

Groups, users and computers:

Name	Active Directory Doma...	Setting
Administrators	realtime-windowsserve...	Deny
Server Operators	realtime-windowsserve...	Deny
Backup Operators	realtime-windowsserve...	Deny
Account Operators	realtime-windowsserve...	Deny
Denied RODC Passwo...	realtime-windowsserve...	Deny
Allowed RODC Passw...	realtime-windowsserve...	Allow

More about the Password Replication Policy

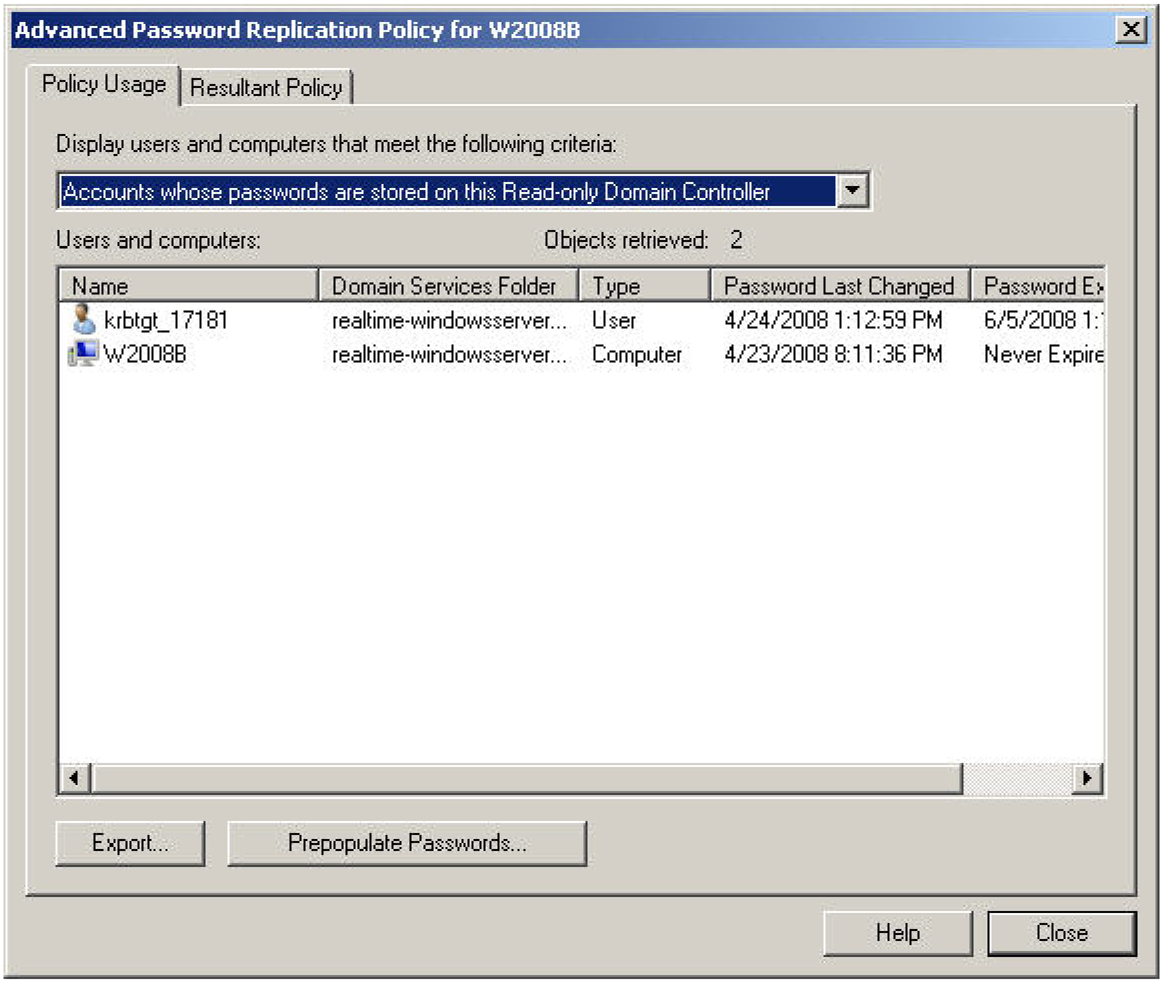
Figure 3: The DCPROMO process includes the initial creation of password replication policy.

☞ As with NTFS permissions, it is a best practice to identify a Global Group for account replication rather than specific users. By default, the Allowed RODC Password Replication Group is created and configured to Allow. The Denied RODC Password Replication Group is a default group that is configured to Deny.

Clicking Next through this screen brings forward the window that we saw in Figure 2. There, you can select which user or group will have local administrator access to manage the RODC. Each of the remaining settings within DCPROMO is similar to those seen in a standard domain controller creation.

Once the RODC has been created, further management of its password replication policy is done through Active Directory Users and Computers. To do so, navigate to the RODC's computer object in Active Directory Users and Computers and choose Properties. In the resulting window, select the Password Replication Policy tab to bring forward a window that looks very similar to what we saw in Figure 3.

This window provides a few additional functionalities if you click Advanced. There, as Figure 4 shows, it is possible to view and export the users and computers whose accounts have been replicated to the local RODC. It is similarly possible to prepopulate passwords associated with those accounts by clicking the *Prepopulate passwords* button. Also possible is the generation of a Resultant Policy report available by selecting the Resultant Policy tab. All these added capabilities are present to further assist you with setting and ensuring that the right accounts are replicated to the RODC.



Advanced Password Replication Policy for W2008B

Display users and computers that meet the following criteria: Accounts whose passwords are stored on this Read-only Domain Controller

Users and computers: Objects retrieved: 2

Name	Domain Services Folder	Type	Password Last Changed	Password Ex
krbtgt_17181	realtime-windowsserver...	User	4/24/2008 1:12:59 PM	6/5/2008 1:
W2008B	realtime-windowsserver...	Computer	4/23/2008 8:11:36 PM	Never Expire

Figure 4: Additional advanced configuration of password replication policy is possible by viewing the properties of the RODC's computer object in Active Directory Users and Computers.

RODCs Protect the Domain

As you can see, RODCs are designed with the specific goal in mind of protecting the domain against the possibility of data disclosure. This additional level of protection is designed to limit the impact of a loss, ensuring that the vast majority of domain accounts remain intact should a single quasi-secured domain controller become lost. If your AD domain includes sites where domain controllers do not have the proper level of physical security, this feature makes Windows Server 2008 a compelling upgrade for its RODC capabilities.