

NT Server Manager: Part II

BY GUY C. YOST

Last month's column explored the first group of features and functions found in NT's Server Manager. This month, I'll wrap up Server Manager so that next month we can delve into setting up user environments with User Manager. Specifically, these remaining items need to be discussed:

- ◆ promoting a BDC to PDC
- ◆ synchronizing the Domain User account database between PDC and BDCs
- ◆ promoting a Backup Domain Controller (BDC)

Recall from previous columns (*Technical Support*, November and December 1997) that a domain can contain at most one PDC, but several BDCs may exist and may also be geographically dispersed. The PDC holds the master copy of the user and group accounts database and replicates this database to all BDCs within the domain. If a PDC fails or becomes inaccessible due to hardware or WAN communications failure, the BDC will continue to validate users into the accessible portion of the domain. To make changes to accounts in the domain, however, a PDC must be present so a BDC may need to be promoted to a PDC. Promoting a BDC to PDC is straightforward: With the BDC highlighted in Server Manager's member list, simply click "Computer" on the main menu bar, and then select "Promote to Primary Domain Controller." Server Manager then asks you to confirm the operation and warns that all connections to the PDC (if available) and BDC will be dropped in the process. See Figures 1 and 2.

The PDC holds the master copy of the user and group accounts database and replicates this database to all BDCs within the domain.

PROMOTING A BDC TO PDC: PROMOTION WARNING

While the promotion process is relatively simple for the administrator, be warned that this process is not seamless to the users on the network. It can take several minutes to complete because the operation first checks to see if the PDC is available and if so, copies the most current database version to the BDC. The PDC is then automatically demoted to BDC while the roles are switched. After the process completes, users can log back into the domain and continue their work. If you click the Help button on the screen illustrated by Figure 2, you'll read about how managing this process via remote access is not supported if either the PDC or BDC affected by the operation is also managing your remote access connection. The verbiage in the message is a little vague, but the bottom line is that this operation is intended to be performed at the console of the PDC or BDC, or from a separate remote access server that will not be affected by the change.

Tip of the Month: Organizations requiring tight security can take advantage of the fact that no changes can be made to the Domain database in the absence of the PDC. School administrators, for example, can make changes to the network at night or weekends.

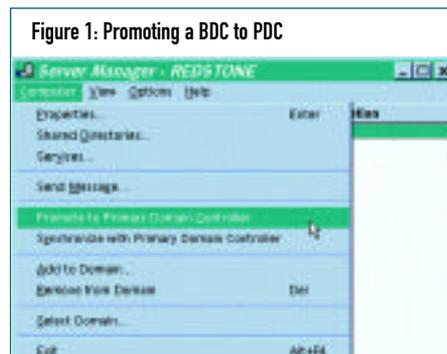


Figure 2: BDC Promotion Warning

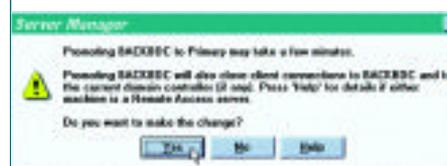
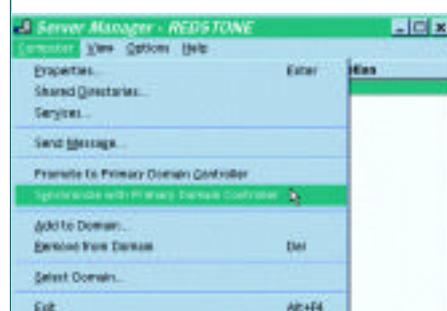


Figure 3: Synchronizing Domain Controllers



When students are on the network, however, the PDC can be made unavailable to the network by simply disconnecting the NIC patch cable. Would-be hackers who may even guess the administrator's password won't be able to change network security due to the PDC's absence.

SYNCHRONIZING THE DOMAIN USER ACCOUNT DATABASE BETWEEN PDC AND BDCS

In normal operation, daily changes will be made to the ACLs (access control

lists) and user account profiles as part of on-going maintenance. By default, changes will automatically propagate every five minutes. The administrator can also force the synchronization between the PDC and BDCs in a couple of ways.

First, the entire domain can be synchronized by highlighting the PDC in the server list

GATE'S GOTCHAS

In the December 1997 issue I stated that NT was not “made for” wide area networking. Here’s another example. I have a client whose single NT domain is spread across two sites. Site 1 contained the PDC and Site 2 had a BDC. The WAN link went down for some time, and the administrator at Site 2 needed to update the account information for users at that site. Consequently, Site 2’s BDC was promoted to a PDC to allow the necessary changes and updates; however, all the while Site 1’s PDC continued to run, and its administrator continued to manage/change Site 1 users’ account information. When the link came up again, the network naturally complained about having two PDCs, so Site 2 was again demoted to BDC. The changes made to Site 2’s BDC (while it was a PDC) were lost. Hopefully this synchronization problem will be addressed in future releases of NT. It is only fair to note that this is not a problem with Novell’s Directory Services, which allows updates to be made to any server’s NDS database in the tree.

window, choosing Computer from the menu bar, and then “Synchronize Entire Domain.” This propagates the current PDC contents to all BDCs. Another approach selectively synchronizes specific BDCs to the PDC. To do this, highlight the desired BDC from the server list window, choose Computer from the menu bar, and then “Synchronize with Primary Domain Controller,” as shown in Figure 3. Notice that the drop-down menu options will change slightly depending on whether you’re working with a PDC or BDC. In either case, the process will take some time depending on the size of the domain (the number of objects in the Domain database). Also, significant network traffic will result from the operation, so performing this action would be best for your users if initiated after-hours.

Next month’s column will examine NT’s User Manager utility and discuss strategies for creating user templates, groups, policies, login scripts, and domain trust relationships. As always, thanks for reading. 



NaSPA member Guy C. Yost is the owner of Redstone Consulting, an IT management consulting firm in New York. He has authored several books on networking for Que Publishing, including Learning NetWare 4.1, and NetWare 4.1 SmartScan, and contributes to Technical Support magazine as an author, columnist and technical editor. Guy also develops and conducts seminars on networking with Windows NT, UNIX, NetWare and Internet/intranet technologies across the United States and Canada. He can be reached at (518) 674-5606 or gyost@logical.net.

©1998 Technical Enterprises, Inc. For reprints of this document contact sales@naspa.net.