

Forcibly Removing Active Directory from a DC Retire a Domain Controller

Daniel Petri

Dcpromo is the Windows 2000 and Windows Server 2003 GUI interface for promoting a server to the role of being a Domain Controller, and if is already a DC, then dcpromo will be the tool to use to demote it back to being a member server. Dcpromo has a specific set of checks it performs before allowing the process to continue. These requirements change based on whether the server is being promoted or demoted. In this article we will deal with demoting issues. Dcpromo might fail when trying to demote a Domain Controller in some cases. These scenarios include, for example:

- There are no domain controllers currently available in the parent domain when you try to demote the last domain controller in a child domain.
- Dcpromo cannot complete because there is a name resolution, authentication, replication engine, or AD object dependency that you cannot resolve.
- A DC has not replicated incoming Active Directory changes in Tombstone Lifetime (Default Tombstone Lifetime is 60 days for Windows 2000 and Windows Server 2003 DCs, and 180 days for Windows Server 2003 SP1 and R2 DCs) number of days for one or more naming contexts.

If you run Dcpromo on an existing DC to demote it and it fails because of one of the above scenarios the best thing you should do is to try to resolve the problem and then restart Dcpromo. However, if Dcpromo still fails you can still demote the DC by running Dcpromo with the /forceremoval switch, which tells the process to ignore errors. Note that the /forceremoval demotion causes the loss of any locally held changes and should be considered a last resort that you should use and only when absolutely necessary.

With /forceremoval, an administrator can forcibly remove Active Directory and roll back the system without having to contact or replicate any locally held changes to another DC in the forest. Note: The /forceremoval switch is only supported on Windows 2000 Servers that either have SP2 with Q332199 hotfix installed on them, or with SP4, and on Windows Server 2003 servers.

Windows Server 2003 SP1 enhances the /forceremoval process. When it is run it checks to determine whether the DC hosts an operations master role (FSMO role – read my “Understanding FSMO Roles in Active Directory” article), is a Domain Name System (DNS) server, or is a global catalog server. For each of these roles, the administrator receives a popup warning that advises the administrator to take appropriate action.

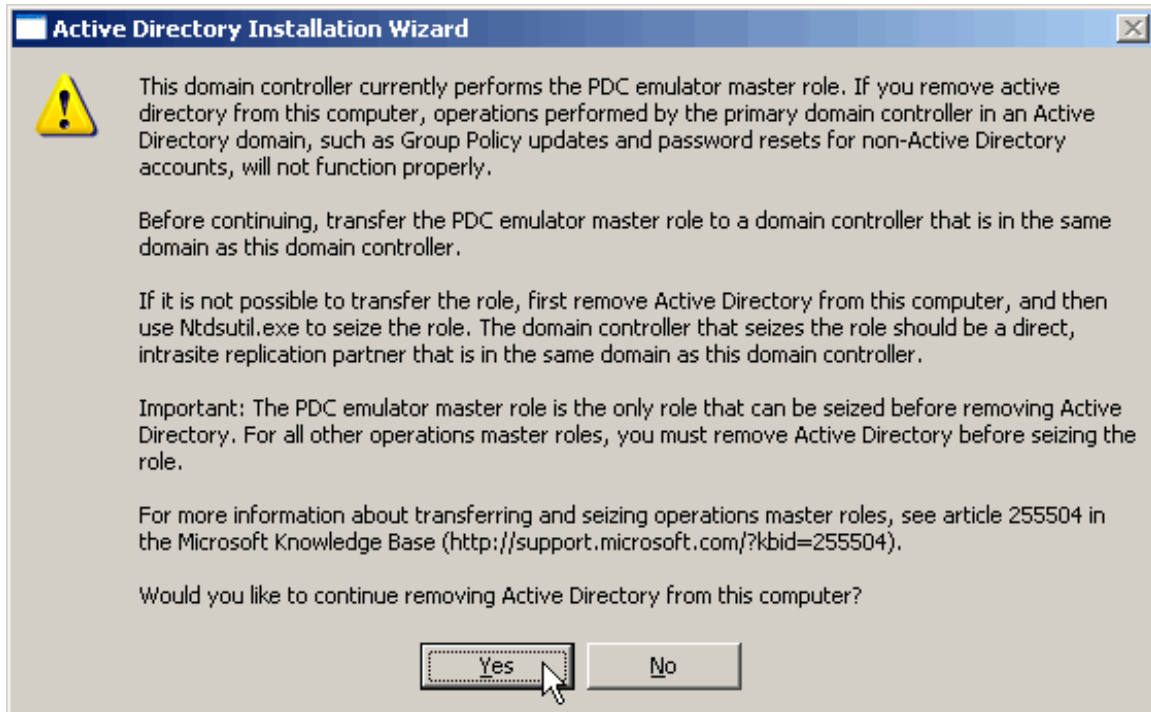
RID Master warning:



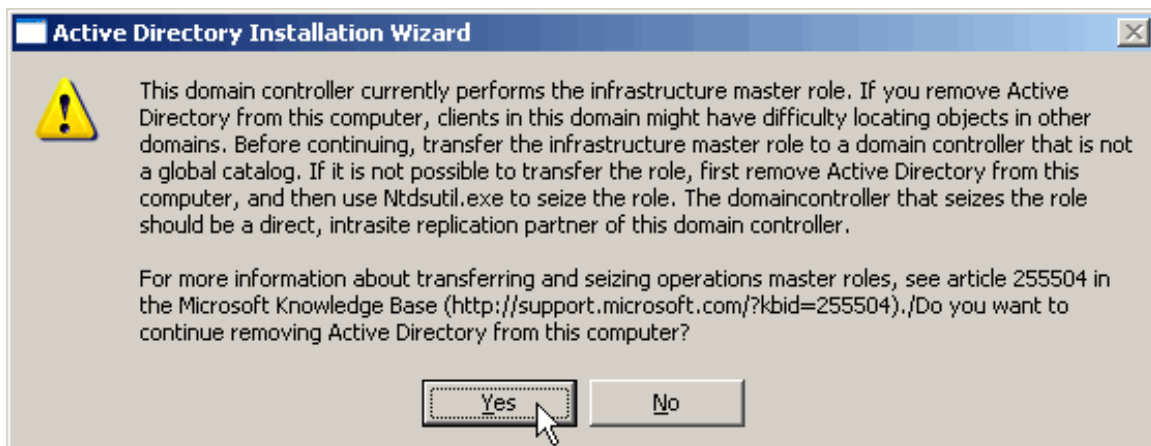
Forcibly Removing Active Directory from a DC Retire a Domain Controller

Daniel Petri

PDC Emulator warning:



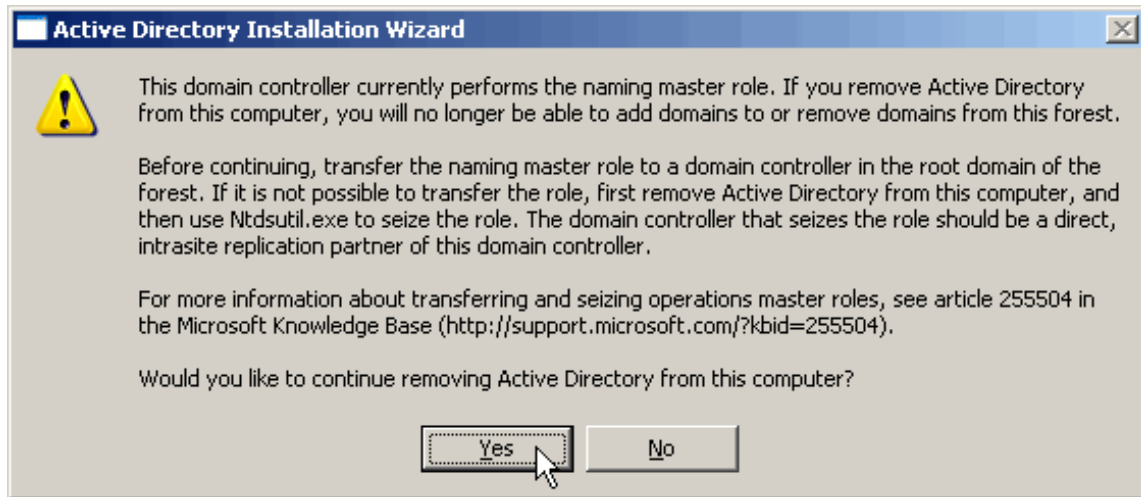
Infrastructure Master warning:



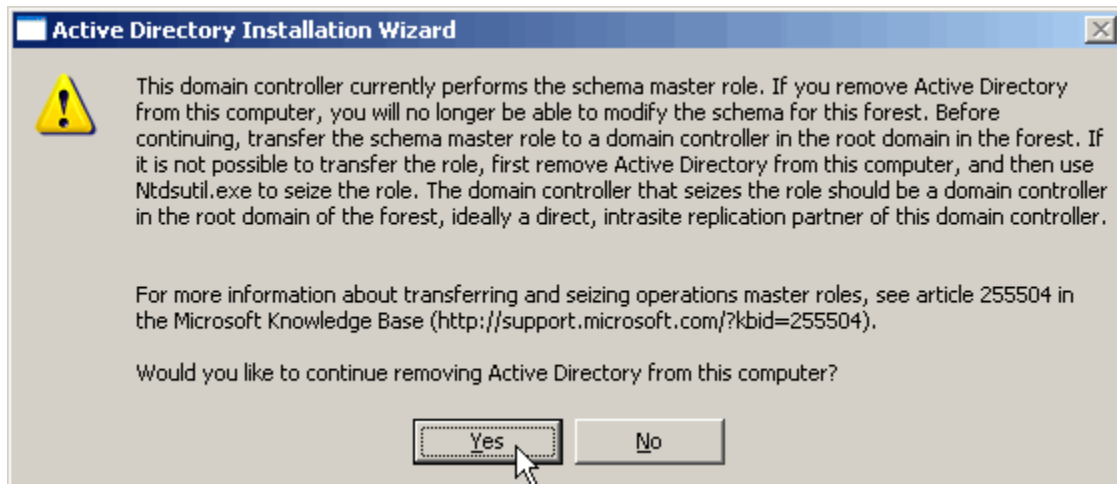
Forcibly Removing Active Directory from a DC Retire a Domain Controller

Daniel Petri

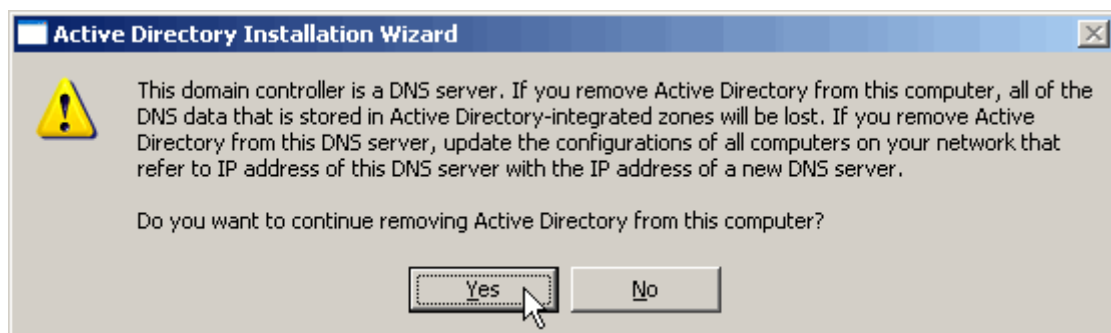
Naming Master warning:



Schema Master warning:



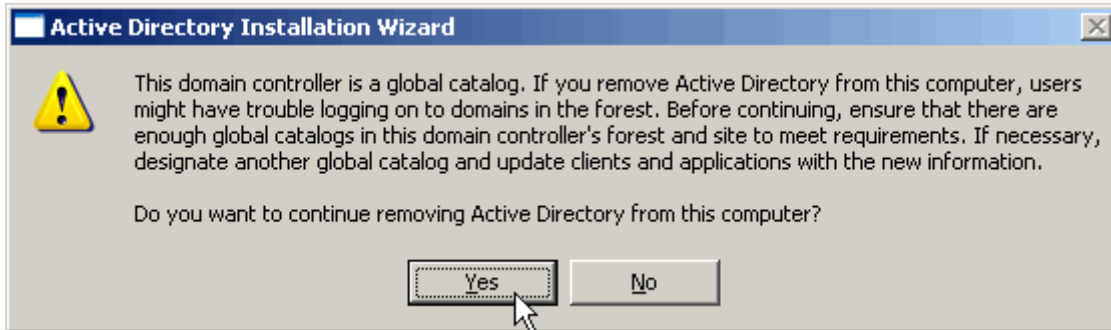
DNS Server warning:



Forcibly Removing Active Directory from a DC Retire a Domain Controller

Daniel Petri

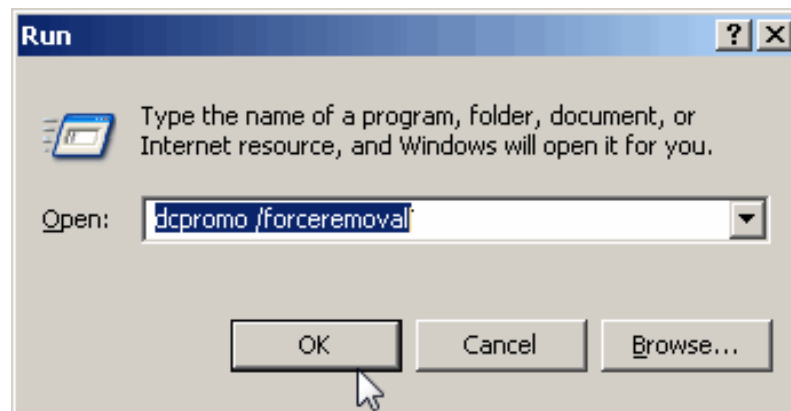
Global Catalog Server warning:



When you force the demotion of a DC, you return the operating system to a state that is the same as the successful demotion of the last domain controller in a domain (service start values, installed services, use of a registry based SAM for the account database, computer is a member of a workgroup). Note: In Windows 2000, the System event log identifies forcibly demoted DCs and instances of the /forceremoval operation by event ID 29234. In Windows Server 2003 the System event log identifies forcibly demoted DCs by event ID 29239.

1. Click Start, click Run, and then type the following command:

```
dcpromo /forceremoval
```

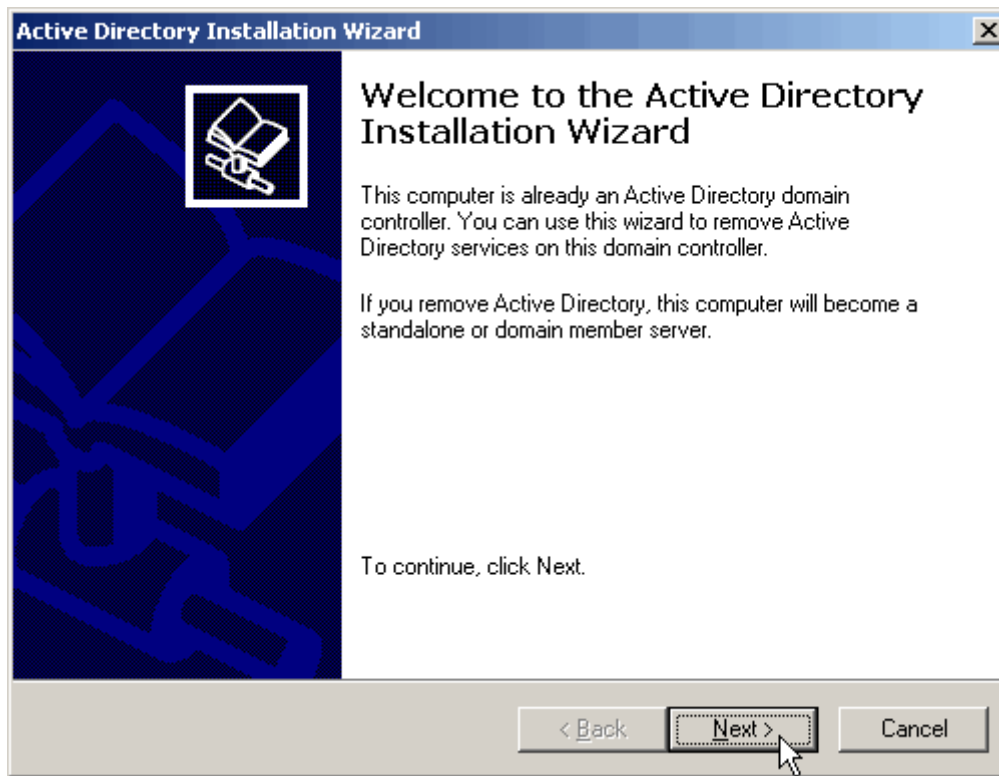


Click Ok.

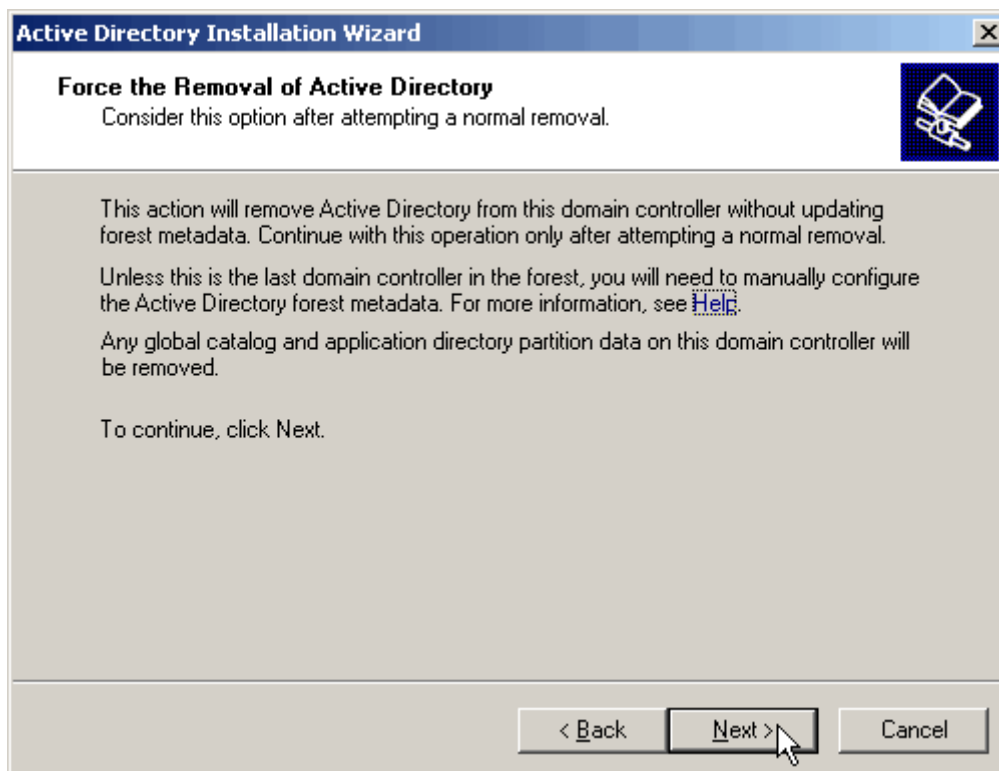
2. At the Welcome to the Active Directory Installation Wizard page, click Next.

Forcibly Removing Active Directory from a DC Retire a Domain Controller

Daniel Petri



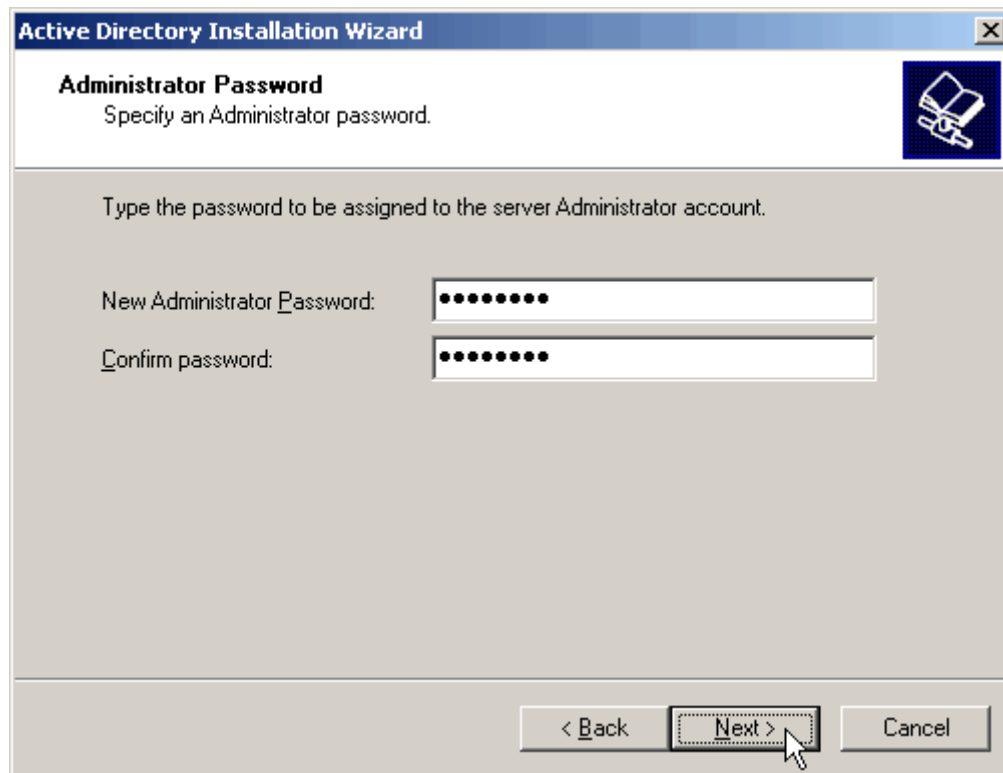
3. At the Force the Removal of Active Directory page, click Next.



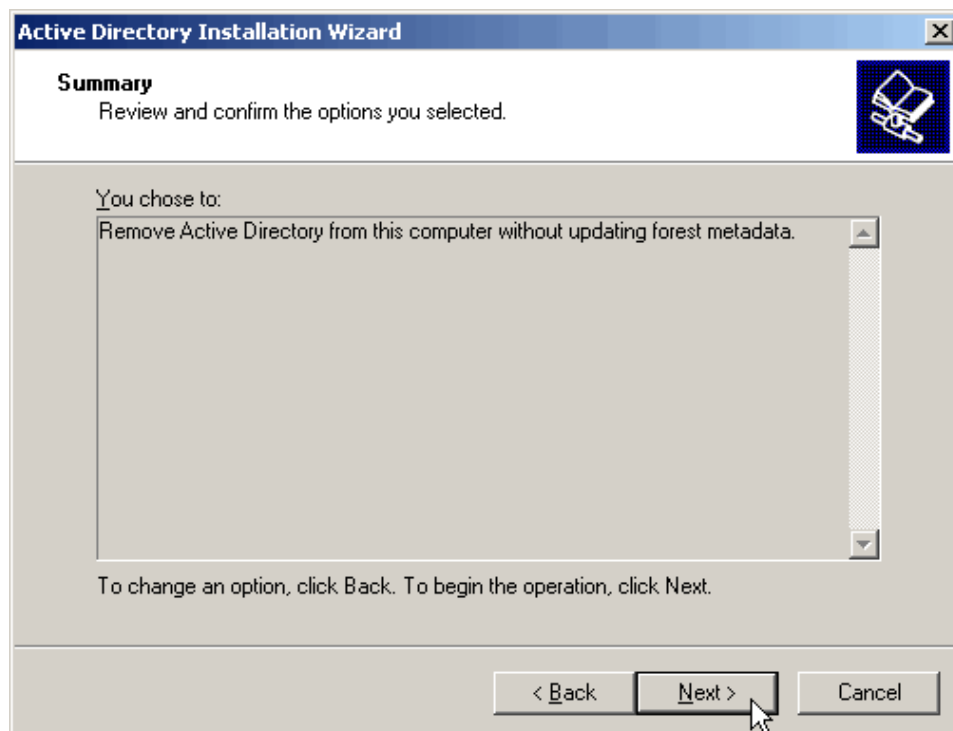
Forcibly Removing Active Directory from a DC Retire a Domain Controller

Daniel Petri

4. In Administrator Password, type the password and confirmed password that you want to assign to the Administrator account of the local SAM database, and then click Next.



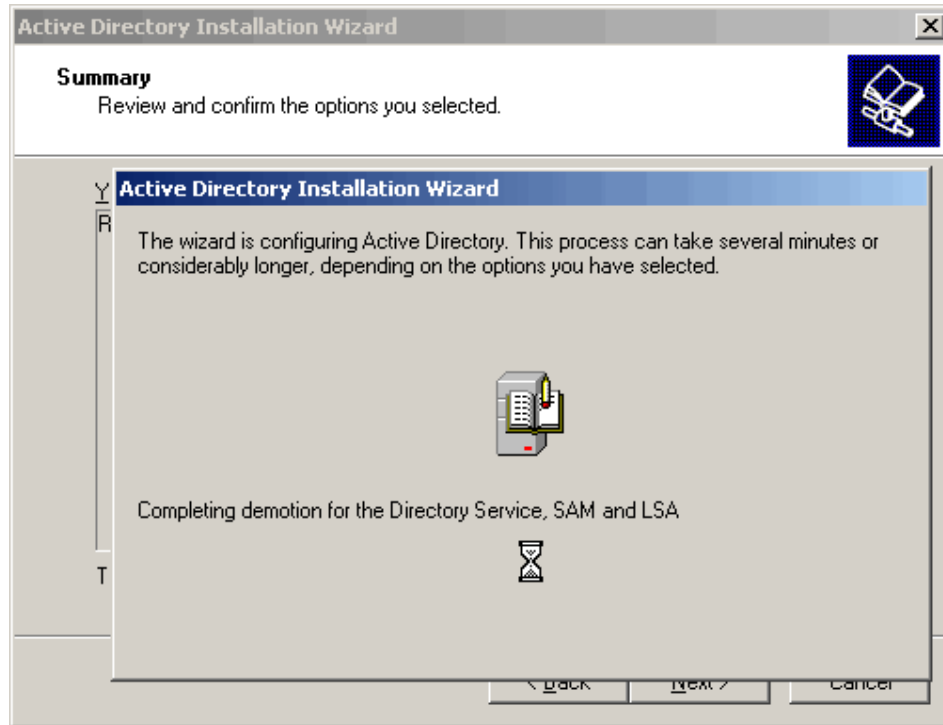
5. In Summary, click Next.



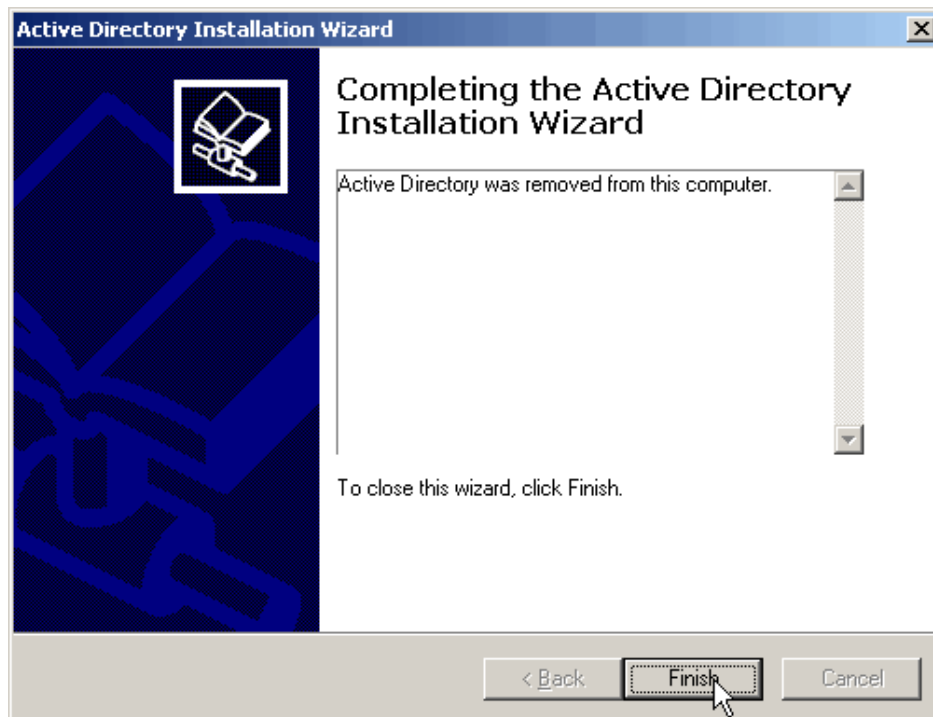
Forcibly Removing Active Directory from a DC Retire a Domain Controller

Daniel Petri

6. Watch as the process runs. Do not disturb it. Go drink some coffee. It should take no longer than a few minutes.



7. When Dcpromo finishes it will prompt you to click Finish.



Forcibly Removing Active Directory from a DC Retire a Domain Controller

Daniel Petri

8. Restart the server.



After you use the `dcpromo /forceremoval` command, all the remaining metadata for the demoted DC is not deleted on the surviving domain controllers, and therefore you must manually remove it by using the `NTDSUTIL` command. For more information please read my "Delete Failed DCs from Active Directory" article ([insert link](#)).