QP2000 - Logging of Detailed Logon Activity

Contents

QP2000 - Logging of Detailed Logon Activity

Purpose of this document and audience

This document describes the operation and maintenance of detailed logging of logon activity that is implemented on the primary domain controller. Server support personnel should be familiar with the operation of detailed logging, the manual maintenance required, and the types of problems that can occur when this feature is enabled.

Revision history

Date of revision	Changes	Made by
20-Feb-2003	Initial release	Felicia King
18-Mar-2003	Remove DRAFT	Felicia King

Definitions

BDC   Backup Domain Controller

DLL   Dynamic Link Library

PDC   Primary Domain Controller

References

189541 - Using the Checked Netlogon.dll to Track Account Lockouts

QP2002 - Recover Group Memberships of Deleted User Account

QP2001 – Central Collection of Netlogon Logs

Process overview

1. Install checked netlogon.dll on the PCD (or BDC) where you want to accumulate detailed event data.

2. Periodically, delete accumulated log files.

Concepts

Netlogon.dll

When you build an NT 4 server, netlogon.dll is automatically loaded.

If you want more detailed information about logon successes and failures (e.g., if you are trying to analyze account lockouts), you must install and configure a "debug-checked" version of netlogon.dll. Microsoft article *189541 - Using the Checked Netlogon.dll to Track Account Lockouts* discusses this DLL file in more detail.

Registry entries for checked netlogon.dll

Proper setup of checked netlogon.dll requires the following DBFlag registry entry:


```
Netlogon
├─ Enum
├─ FullSync
├─ Linkage
├─ Parameters
└─ Security
```

```
DBFlag : REG_SZ : 0x20000004
DisablePasswordChange : REG_DWORD : 0
Scripts : REG_EXPAND_SZ : %SystemRoot%\system32\repl\export\s
TrustedDomainList : REG_MULTI_SZ : S
Update : REG_SZ : no
```

Log of logon information

Detailed logon information is written to **C:\WINNT\debug\netlogon.log**. Maximum file size is 19 MB.

- When the checked netlogon.dll detects that the log has reached maximum size, it renames it **netlogon.bak** and begins a new log.

- When that new log reaches 19 MB, it overwrites the netlogon.bak file and begins a new log. Since at any given time, only one .log and one .bak file exist, the maximum amount of space that the .log and .bak files take up is 38 MB.

Batch file to archive previous log files

To study account lockout problems, we created a batch file (**CopyNetlogon.bat**) that:

- Moves each .bak file to an archive folder on the D:\ drive of the PDC (**\\PDCName\d$\Netlogon.logArchive**)

- Renames it as a sequentially numbered (001 – 999) file, and

- Restores the .log extension

A copy of this batch file is available in the source files location.

Example of archived log files on the PDC:
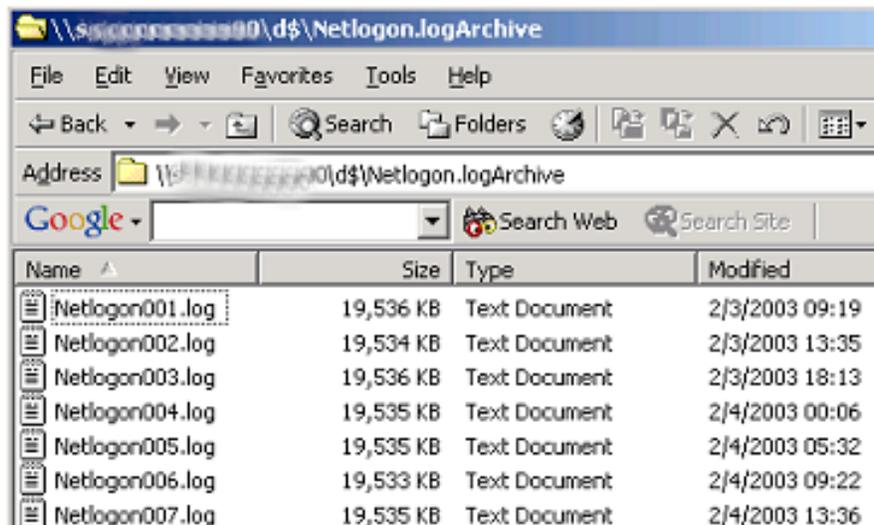
Name	Size	Type	Modified
Netlogon001.log	19,536 KB	Text Document	2/3/2003 09:19
Netlogon002.log	19,534 KB	Text Document	2/3/2003 13:35
Netlogon003.log	19,536 KB	Text Document	2/3/2003 18:13
Netlogon004.log	19,535 KB	Text Document	2/4/2003 00:06
Netlogon005.log	19,535 KB	Text Document	2/4/2003 05:32
Netlogon006.log	19,533 KB	Text Document	2/4/2003 09:22
Netlogon007.log	19,535 KB	Text Document	2/4/2003 13:36

Scheduled task calls batch file

A scheduled task periodically checks **C:\winnt\debug** for the presence of the netlogon.bak file. (The current period is every 15 minutes.) If it finds one, it launches the CopyNetlogon.bat file. The frequency with which these files are generated reflects the activity on the PDC and may point to a problem if they are more numerous than usual.

Data gathering on PDC

Although the checked netlogon.dll can be installed on any NT 4 BDC, and we assume it is currently installed on all BDCs, this document describes how the data gathering occurs on the PDC.

Note: This particular netlogon.dll file applies only to NT 4 servers. Windows 2000 and higher servers have built-in detailed logging of logon events. You set a registry entry, then stop and start Netlogon service to launch detailed logging.

Manual cleanup of archive folder

As the archived .log files accumulate, they can easily use up all the space on the PDC D:\ drive. The PDC has 4 GB of space available, but 999 archived .log files consume 19 GB of space; 52 log files take up 1 GB of space.

To avoid the problems that running out of space can cause (for example, the program that recovers group memberships requires space for the large text file that it produces), someone must manually clean out the accumulated archive logs from time to time. Although GMSE never knows in advance when it might need the archived files to investigate some event, the negative consequences of letting files eat all available space outweigh the small probability that the files might be needed right after you delete them.

Note: In the future, the batch file will be modified to clean out accumulated files, but the process is currently a manual one.

Assumptions

This document assumes that you have authorization to delete files on the D:\ drive of the PDC.

Before you start

Obtain a copy of the debug version of netlogon.dll from Microsoft or another source. Use the version for Service Pack 6a.

Procedures

Install checked netlogon.dll

1. In folder **C:\WINNT\System32**, rename the existing (original) netlogon.dll file, e.g., call it **netlogon.orig**.

2. Copy the new checked netlogon.dll file to **C:\WINNT\System32**.

3. Configure the required DBFlag registry entry.
    You can do this manually, or you can run the appropriate command file. The source file contains file NetlogonReg.cmd that you can use for this purpose. Example of a command:

    NetlogonReg.cmd *server_list*

    Where *server_list* is a text file with the names of the servers whose DBFlag registry entries you want to set.

    Note: This command file changes only DBFlag and leaves all other registry entries intact.

4. Reboot the server.
    Note: You must reboot the server to make the change effective.

Manually delete accumulated log files

1. Ensure that no investigation is in progress that might require the accumulated data in the log files.

2. Open **\\PDCName\d$\Netlogon.logArchive**.

3. Delete files as you wish.

CAUTION! Look carefully at the date/time stamps of the files that you delete. Depending on what was previously deleted, the batch file may restart the file numbering at 001 for more recent log files. Thus higher-numbered files may be older than lower-numbered files. Example:

Name △	Size	Type	Modified
Netlogon007.log	19,536 KB	Text Document	2/19/2003 1
Netlogon008.log	19,535 KB	Text Document	2/19/2003 1
Netlogon009.log	19,533 KB	Text Document	2/19/2003 1
Netlogon010.log	19,536 KB	Text Document	2/19/2003 1
Netlogon011.log	19,532 KB	Text Document	2/19/2003 2
Netlogon012.log	19,536 KB	Text Document	2/20/2003 0
Netlogon013.log	19,532 KB	Text Document	2/20/2003 0
Netlogon014.log	19,534 KB	Text Document	2/20/2003 0
Netlogon068.log	19,532 KB	Text Document	2/16/2003 0
Netlogon069.log	19,536 KB	Text Document	2/16/2003 1
Netlogon070.log	19,533 KB	Text Document	2/16/2003 1
Netlogon071.log	19,533 KB	Text Document	2/16/2003 2
Netlogon072.log	19,537 KB	Text Document	2/17/2003 0