

QP2001 - Central Collection of Netlogon Logs

Contents

QP2001 - Central Collection of Netlogon Logs	1
Purpose of this document and audience	1
Revision history	1
Definitions	1
References.....	2
Process overview	2
Concepts	2
Archiving of netlogon.bak files	2
Limited space on DCs.....	2
Central storage of backup files	3
Software configuration of servers.....	4
Utilities required	6
Archive on central server.....	6
Assumptions.....	7
Before you start.....	7
Procedures.....	7
Get current list of BDCs	7
Install checked netlogon on all BDCs.....	8
Schedule an archive check every hour.....	9
If needed, turn off detailed logging	10
Periodically delete old .zip files.....	10
Unzip files that you want to investigate.....	10

QP2001 - Central Collection of Netlogon Logs

Purpose of this document and audience

This document describes how logs from the detailed logging of logon activity on domain controllers in a Windows domain (NT 4 or Active Directory) are stored in a central server archive for reference. Server support personnel should be familiar with the operation of detailed logging and the archive of past logs.

Revision history

Date of revision	Changes	Made by
20-Mar-2003	Initial release	Felicia King

Definitions

BDC	Backup Domain Controller
DC	Domain Controller
DLL	Dynamic Link Library
PDC	Primary Domain Controller

References

Task Scheduler and AT Account Issues

Logging of Detailed Logon Activity

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

Process overview

1. Create a current list of Domain Controllers and delete all extraneous text.
2. Install checked netlogon.dll on all DCs.
3. Copy the required files to each DC.
4. On the central archive server, use Task Scheduler to schedule an hourly check for a .bak file existence and perform the archiving.
5. Periodically, manually delete accumulated log files on the central server.

Concepts

Archiving of netlogon.bak files

If detailed logging of logon events is enabled on a Domain Controller, eventually the log file expands to its maximum size (19 MB) and is written to a backup file. When the log file again reaches its maximum size, this backup file is overwritten.

If domain admins or another support group has to investigate a problem, it is often useful to have more than one backup file from which to extract historical data.

Limited space on DCs

Some of the existing DCs have limited storage space and/or no D:\ drives. So accumulating multiple backup files locally is not an option. Detailed logon information is limited to the current .LOG file and the .BAK file.

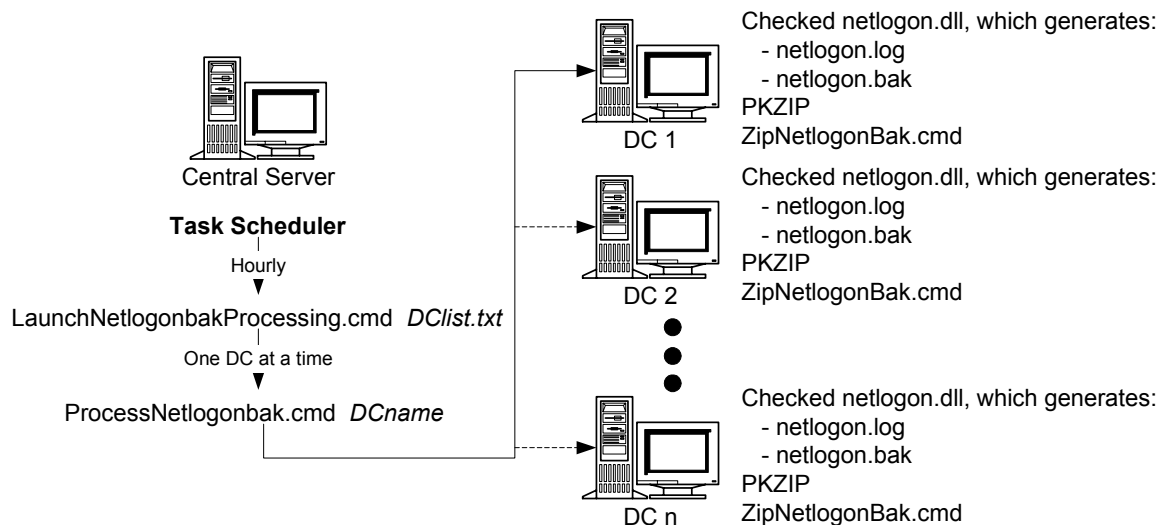
A solution is required that archives the .BAK file periodically to a server that has enough space to store the information for multiple DCs.

Central storage of backup files

The design for detailed log file storage involves the following main elements:

- A central server with the space for log files and with a scheduled program that hourly:
 - checks for the existence of a netlogon.bak file on each DC
 - Note:** The existence of the .bak file triggers action. If the file does not exist, the script goes on to the next server.
 - runs a script that zips and deletes the .bak file locally on the DC
 - copies the .ZIP file to the central storage area
 - renames it to include server name and a sequential identification number
 - deletes the now archived .ZIP file from the DC server
- Domain Controllers with:
 - debug checked netlogon.dll for detailed logging of logon events
 - a copy of the PKZIP 2.50 compression program
 - a copy of a script for zipping and deleting .bak files

A pictorial representation of relationships is as follows:



Software configuration of servers

The following table shows what resides in each server. All scripts, .exe files, and checked netlogon.dll are available on the Quality Plus website through the source files link. Note that the download package name will match the article number.

Central Server	Domain Controllers
ExtractBDC.exe BDCListFull.txt BackupOrigDLLFiles.cmd CopyOutNetlogon.cmd NetlogonReg.cmd CycleNetlogon.cmd AuditNetlogonGen.cmd CopyOutNetlogonZipStuff.cmd LaunchNetlogonbakProcessing.cmd ProcessNetlogonbak.cmd	Checked netlogon.dll PKZIP.EXE version 2.50 ZipNetlogonBak.cmd Note: Netlogon.dll automatically generates the following files: Netlogon.log (19 MB maximum) Netlogon.bak (19 MB maximum)

The following table describes each software element in more detail:

File and parameters	Description
ExtractBDC.exe <i>netdombdes.txt >BDCListFull.txt</i>	Extracts just the server names from the list (text file) of BDCs produced by the netdom bdc command.
BDCListFull.txt	The current list of BDCs, one BDC name to a line, cleaned of all other text that netdom produces.
BackupOrigDLLFiles.cmd <i>BDCListFull.txt</i>	Renames the standard netlogon.dll file in each NT 4 BDC in the input list to netlogon.orig . The standard netlogon.dll file is installed in folder C:\WINNT\System32 during the standard server build.
CopyOutNetlogon.cmd <i>BDCListFull.txt</i>	Copies the checked version of netlogon.dll to folder C:\WINNT\System32 on all NT 4 BDCs in the input list.
NetlogonReg.cmd <i>BDCListFull.txt</i>	Sets the Netlogon DBFLAG registry value to 0x20000004 on all servers in the input list. This DBFLAG value is required for checked netlogon.dll. By changing the .cmd, file you can reset DBFLAG to zero, which effectively disables log generation on the servers.
CycleNetlogon.cmd <i>BDCListFull.txt</i>	Stops and starts netlogon service on the servers in the input list. The .cmd file uses the rcmd command to perform the stop/start locally, which is much more efficient and less time consuming than doing it remotely via a netsvc or sc command. The cycling is done on just one server at a time so that only one BDC is unavailable at a time.

File and parameters	Description
AuditNetlogonGen.cmd <i>BDCListFull.txt</i>	Checks that netlogon.log is being generated in folder C:\WINNT\Debug on all servers in the input list.
CopyOutNetlogonZipStuff .cmd <i>BDCListFull.txt</i>	Copies PKZIP.EXE and ZipNetlogonBak.cmd to folder C:\WINNT\Debug on all servers in the input list. The \Debug folder is created during installation of checked netlogon.dll.
LaunchNetlogonbakProcessing .cmd <i>BDCListFull.txt</i>	Script that you schedule via Task Scheduler to call ProcessNetlogonbak.cmd for one server at a time. Servers to process are in the input list.
ProcessNetlogonbak.cmd <i>servername</i> Note: LaunchNetlogonbakProcessing. Cmd feeds server names to this script one server at a time.	<ul style="list-style-type: none"> • Checks the server's C:\WINNT\Debug folder for the existence of a netlogon.bak file. • If it exists, schedules ZipNetlogonBak.cmd on the remote server to zip the .bak file and delete the .bak file. • Copies the zipped .bak file (now a .zip file) to the central server and renames it by adding the server name and an incremental ID. • Deletes the .zip file from the remote server. Note: This file uses the AtNow utility.
PKZIP.EXE -exx netlogon.zip netlogon.bak Note: The ZipNetlogonBak.cmd script calls this program.	Zips the specified file. Version 2.50 offers a high-compression parameter (-exx) that makes files extremely compact.
ZipNetlogonBak.cmd	<ul style="list-style-type: none"> • Checks if a netlogon.bak file exists. If not, exits. • If the .bak file exists, calls PKZIP to zip it and deletes the .bak file.

Utilities required

The command files depend on the availability of the following utilities:

AtNow	Schedules programs and commands to run in the near future. Available for free at http://nirsoft.multiservers.com/utills/atnow.html . As used in this application, the command schedules the ZipNetlogonBak.cmd script 60 seconds from now (which is the smallest usable future time increment). The script gives PKZIP 120 seconds to finish zipping the 19-MB .bak file.
PKZIP 2.50	Zips files (in this case, the netlogon.bak files) at a high compression rate. Note: PKZIP and PKUNZIP do <i>not</i> support file names longer than 8 characters plus the extension. See http://www.pkware.com/ for purchase information.
Reg.exe	Sets a specific registry entry without changing anything around it. Available from the NT Resource Kit.
Rcmd	Remote Command: Connects remotely to a server. Available from the NT Resource Kit.
Sleep.exe	Wait (sleep) for the specified amount of time. Available from the NT Resource Kit.
WZUNZIP	Part of a command-line version of WinZip. It requires a separate installation.

Archive on central server

The \NetlogonLogs folder on the central server holds the archived logs. Example of archived logs:

Name	Size	Modified
PRSNJNFONetlog001.zip	1,455 KB	2/19/2003 1:01 AM
PRSNJNFONetlog002.zip	1,422 KB	2/20/2003 9:54 AM
PRSNJNFONetlog003.zip	1,408 KB	2/24/2003 1:00 AM
PRSNJNFONetlog004.zip	1,428 KB	2/27/2003 1:00 AM
PRSNJNFONetlog005.zip	1,425 KB	2/28/2003 1:00 AM
PRSNJNFONetlog006.zip	1,425 KB	3/3/2003 1:00 AM
PRSNJNFONetlog007.zip	1,415 KB	3/5/2003 1:01 AM
SCJCPARBUENO507Netlog001.zip	1,432 KB	2/20/2003 10:03 AM
SCJCPARBUENO507Netlog002.zip	1,325 KB	2/24/2003 1:03 AM
SCJCPARBUENO507Netlog003.zip	1,416 KB	2/27/2003 1:03 AM
SCJCPARBUENO507Netlog004.zip	1,413 KB	2/28/2003 1:03 AM

The date/time stamp shows when the copy to the central server occurred, not when the archive was written. There may be as much as a 2-hour difference between the times.

Not every server has a .zip files in the archive. If a BDC is not logging many events due to low activity on the server, it may not produce a .bak file for a long time. It's the presence of a netlogon.bak file that triggers the archiving.

Assumptions

This document assumes that you have:

- Domain admin rights
- Access to the source files and the utilities (e.g., rcmd, netdom) described in this document
- Knowledge of Task Scheduler (see document *QP0001 - Task Scheduler and AT Account Issues* for more information)
- An understanding of the information in *QP2000 - Logging of Detailed Logon Activity*

Before you start

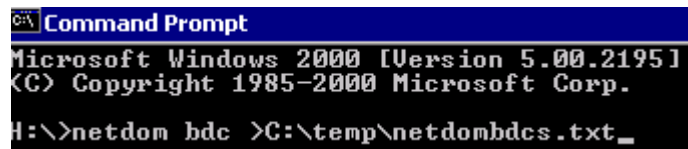
Ensure that:

- NTReskit is installed on every server where the scheduled task is configured.
- AtNow.exe is in the search path of the server where the scheduled task is configured.

Procedures

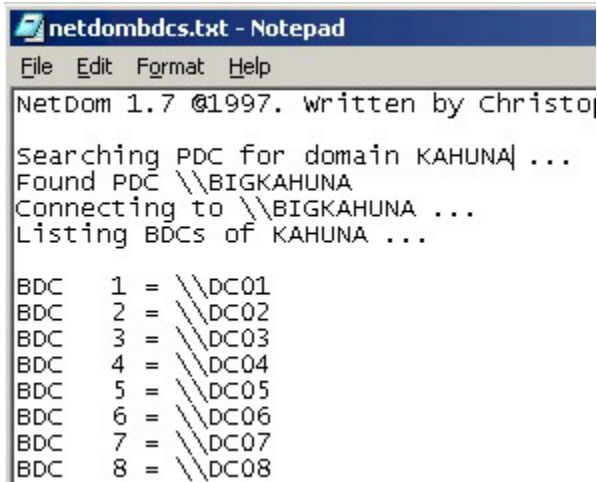
Get current list of BDCs

1. From the command prompt, run the netdom command. Example:



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
H:\>netdom bdc >C:\temp\netdombdcs.txt_
```

Result: The BDC servers appear along with other information. Example:



```
netdombdcs.txt - Notepad
File Edit Format Help
NetDom 1.7 @1997. written by Christof
Searching PDC for domain KAHUNA ...
Found PDC \\BIGKAHUNA
Connecting to \\BIGKAHUNA ...
Listing BDCs of KAHUNA ...

BDC 1 = \\DC01
BDC 2 = \\DC02
BDC 3 = \\DC03
BDC 4 = \\DC04
BDC 5 = \\DC05
BDC 6 = \\DC06
BDC 7 = \\DC07
BDC 8 = \\DC08
```

2. Clean up the list so that only server names appear:

```
ExtractBDC.exe netdombdcs.txt >BDCListFull.txt
```

Install checked netlogon on all BDCs

1. You cannot delete netlogon while it operates on a server. You first rename it with the following script:

```
BackupOrigDLLFiles.cmd BDCListFull.txt
```

2. Run the script that copies checked netlogon to all BDCs:

```
CopyOutNetlogon.cmd BDCListFull.txt
```

3. Set the registry entry for checked netlogon.dll on all BDCs:

```
NetlogonReg.cmd BDCListFull.txt
```

4. Ensure that **rcmd** (remote command server) is on all BDCs.
5. Reboot all BDCs.

Result: The C:\WINNT\Debug folder is created for netlogon logs.

6. After 5 minutes, run an audit to ensure that checked netlogon is creating log files:

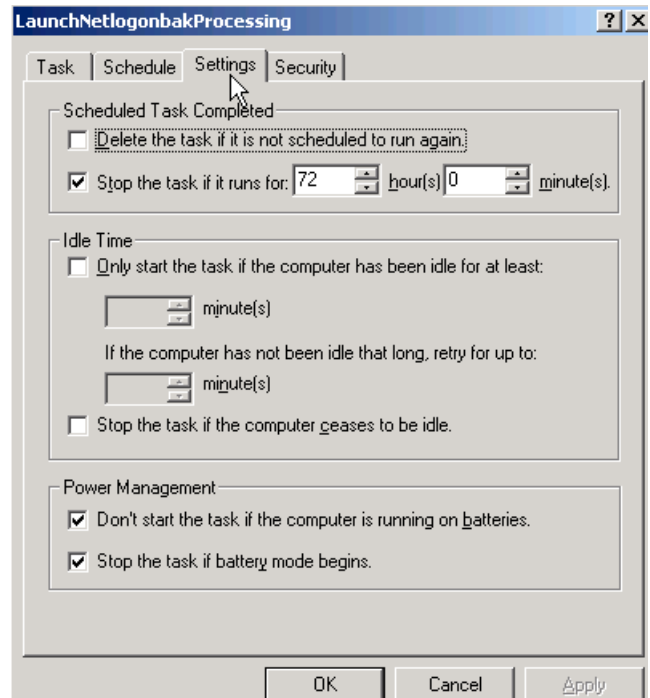
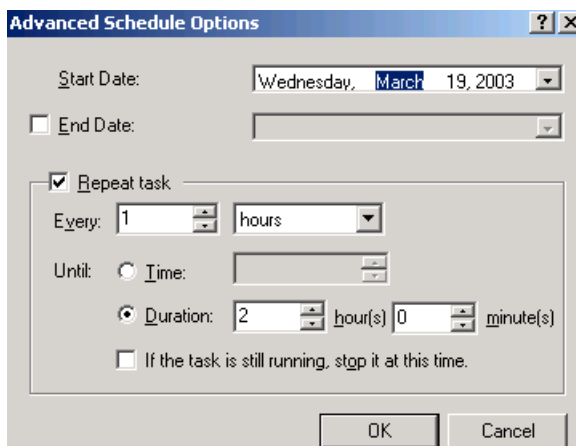
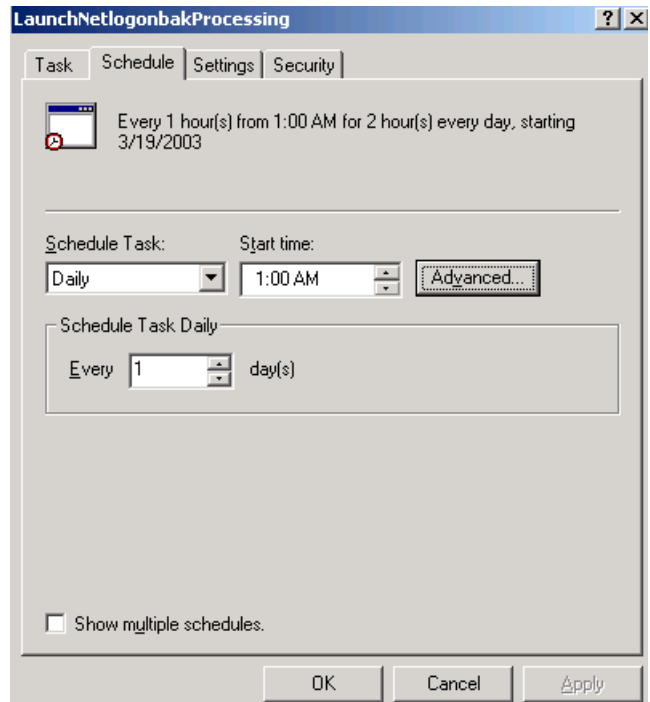
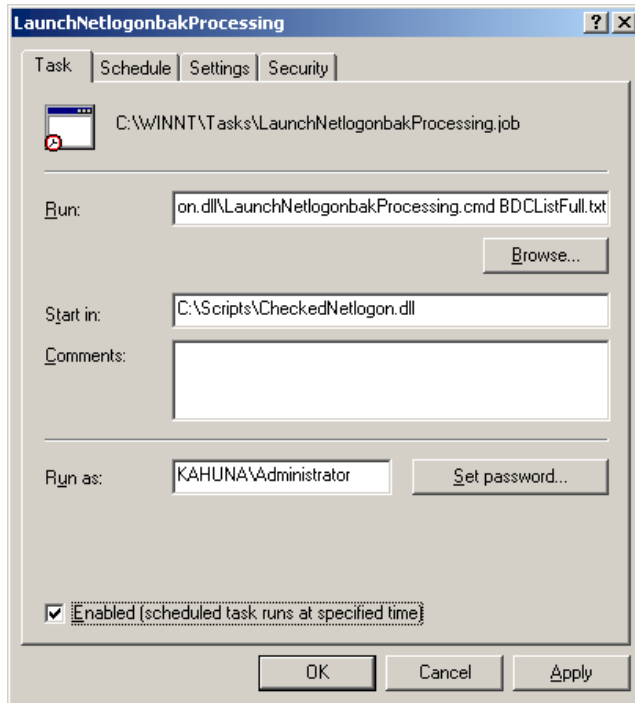
```
AuditNetlogonGen.cmd BDCListFull.txt
```

7. Copy the PKZIP and ZipNetlogonBak.cmd files to all BDCs:

```
CopyOutNetlogonZipStuff.cmd BDCListFull.txt
```

Schedule an archive check every hour

Use Task Scheduler to run an archive check every hour around the clock and specify Domain Admin credentials. Schedule setup is as follows:



If needed, turn off detailed logging

You may want to disable detailed logging to remove the (small) load it places on the server.

1. In the **NetlogonReg.cmd** file, change the DBFlag registry entry to **0** (zero).
2. Save the file as some other name.
3. Run the file.
4. Stop and start netlogon service:

CycleNetlogon.cmd BDCListFull.txt

Periodically delete old .zip files

Eventually, the accumulation of zipped netlogon.bak files will use all the space available on the central server. Delete old files as you wish.

Note: Always watch the date/time stamp of the file that you are deleting. After you delete files over time, the sequential ID may no longer indicate relative age—unless you deleted *all* accumulated files for a BDC at one time.

Unzip files that you want to investigate

When you need to unzip a group of archived log files:

1. Copy **UnzipFiles.cmd** from the source files to the folder where you have all the files that you want to unzip.
2. Remove any .ZIP files that you do *not* want to unzip.

Result: The folder contains UnzipFiles.cmd and all the files to be unzipped.

3. Run **UnzipFiles.cmd**.

Result: All .ZIP files in the folder are unzipped to a file of the original name except with a .LOG extension. The original .ZIP files remain unaltered.