Release 3 Update 3 Service Document

This document includes information that was not included with the product documentation, or includes diagnostic steps that a customer would not need for normal operation. It is written with the intent of being distributed to IBM service and technical marketing personnel.

Read Me's

This is a list of the Documentation included on the CD. The most current information about any of the individual components is included in these.

IBM Network Station Manager Product Information

x:\ntnsm\en\Readme.txt

x:\ntnsm\en\pubs\readme.txt

x:\ntnsm\en\utility

eNetwork On Demand Product Information

x:\ntnsm\en\products\enod\ndis\read.me

x:\ntnsm\en\products\enod\tcpip\readme.txt

Third Party Installation Information

x:\ntnsm\en\products\adobe\readme.txt

x:\ntnsm\en\products\lotusgo\readme.txt

x:\ntnsm\en\products\netscape\readme.txt

x:\ntnsm\en\products\Citrix\readme.txt

x:\ntnsm\en\products\Ncd\readme.txt

IBM Network Station Manager and optional products

IBM Network Station Manager now ships with trial versions of Citrix Metaframe and NCD Wincenter UIS. Both of these products require Microsoft Windows NT Server 4.0, Terminal Server Edition. They will not run on Microsoft Windows NT Server.

Citrix Metaframe:

Allows customers to run Windows-based applications remotely from net workstations.

Requires Microsoft Windows NT 4.0, Terminal Server Edition.

Uses ICA protocol.

Requires either Citrix Metaframe Terminal license or Citrix Metaframe PC license.

NCD WinCenter UIS:

Allows customers to run Windows-based applications remotely from net workstations.

Requires Microsoft Windows NT 4.0, Terminal Server Edition.

Requires Citrix Metaframe.

Uses X11 protocol.

Requires Citrix Metaframe PC license.

Please see the Install and Use document for more information on these products.

Tools

Utility to remove NSM Release 2

In a dual server migration from a NSM Release 2 Primary Domain Controller to a NSM Release 3 Stand Alone Server there is utility to remove NSM release 2 and all its associated products from the Primary Domain Controller. This tool is to be run only after the new server is running and all users have been migrated. It will remove eSuite (preserving the registry files), NSM release 2 (preserving the NSM groups), NSM service packs 1 and 2, Navio Browser, Spyglass browser, IBM TCP\IP services, and the driver for DHCP support. It is located on the CD in x:\ntnsm\en\utility\ntnsmrr2.exe.

Network Station reboot application

A new application is included on the CD called nsreboot.exe. This utility allows administrators to reboot Network Stations from the server. The path is \ntnsm\en\utility\nsreboot.exe. Instructions for use are located in \ntnsm\en\utility\nsreboot.txt.

Service Tool

The service tool gathers system information and diagnoses problems with Network Station Manager on an NT Server.

The tool may be run in one of two ways (CGI recommended):

Running as a CGI:

Web browser address: http:\\(servername)\networkstation\cgi\service.exe

You will be prompted for an administrative user name and password

Running from a DOS prompt:

Displaying to screen: ntnsmver

Output to file: ntnsmver > output_file _name

The tool has 8 main categories:

Web Server Environment Variables	Displays environment variables set by Lotus Go or IIS
Hard Disk Information	Displays available disk space, file system type, and NT Server type.
Registry Entry Settings	Displays NSM registry settings, name of server, domain, and if server is TSE.
List of Running Services	Displays all services running on server.
Network Port Status	Displays which network ports are being used on the server.
TCP\IP Information	Displays type of network card and all TCP/IP configuration information.
User Information	Displays all groups and users on server.
Binary file information	Displays version of NSM files installed.

Note: At this time only 110 users will be listed when this tool is run. If more users are present on the server only the first 110 are displayed. This will be addressed in a future release.

Install Flags

The following flags can be used when running setup from a command line. These can only be used with the CD version of NSM, they will not work on the download version.

"/ndis"

This flag will tell setup not to automatically install the current version or uninstall previous versions of the Intermediate Driver. It will bring up the network control panel so this can be done manually.

"/nsmall"

This flag will install all server locales. NSM will use the default system locale.

“/np”

This installs without checking or configuring the web server, browser, and does not create the NSM shortcut on the desktop. For examples please see the “Full-Screen Solutions” document at http:\\rchasa24.rchland.ibm.com\nstation\pub.htm.

“/as”

This installs a dedicated Authentication Server. This is used for separating the Boot and Authentication Servers. By default the Authentication Server will also be the Configuration Server. This is a full install with the following lines added to the defaults.dft file.

“set exec-startup-commands ={

{mcuis}

{”actlogin-authserve AUTHENTICATION-SERVER-ADDRESS”}

}”

This switch replaces “ AUTHENTICATION-SERVER-ADDRESS” with the fully qualified domain name of the server. If install cannot open the defaults.dft file the generic error message will be given. This does not disable the Authentication Server in any way, but the line will have to be added to defaults.dft manually. If install fails to write the above line with a valid host name there is no error message. The line will be written out exactly as above and the user must substitute the appropriate name. A standard NSM server can be made into an Authentication Server by manually adding these lines. For more information see the “Installation and Use” document.

“/asf”

This forces the Authentication Server install when NSM had previously been installed as a standard server.

“/bs”

This installs only the client portion for a Boot Server after an Authentication Server has been setup. The client binaries and TCP/IP services will be installed but not NSM or the Network Station Login Services.

Panic Uploads

TFTP cannot upload a panic dump from a Network Station with memory greater than or equal to 32 megs. Uploads via NFS are recommended. In a dual server environment the file will be uploaded to the boot server.

1. Go to the nstation\prodbase\service directory.
2. Create a new text file and name it with the last eight digits of the MAC address.
3. Rename this file with a .dmp extension
4. At the client you can now type UN to begin the upload.

Capturing client information

From a console log:

Open a command prompt and type **telnet x.x.x.x 5998**, where x.x.x.x is your network station IP address. If the NT telnet window is too small to capture the whole console, go to Terminal->Preferences... and make your buffer size larger, for example 2000. You can also go to Terminal->Start Logging... to write the information to a file.

Environment information:

Open a command prompt and type **telnet x.x.x.x 5999**, where x.x.x.x is your network station IP address. When prompted for a password, type in **public**. From the telnet prompt, type **get all**.

NT Server Dump Examine Tool

If a server displays a blue screen it is possible to get useful information from the server dump files. To do this you need to make sure that you have the correct symbol tables on the machine before running this utility.

The support\debug\i386 directory has a sub directory called symbols. The dump exam call should look like:

dumpexam -v -y x:\support\debug\i386\symbols -f<output filename> <memory dump file>

Where x: is the CD-ROM drive with the NT server install CD in it. If any service pack has been applied, the symbol directory from the service pack (same directory path) should be used. Dumpexam.exe can be obtained from the NT Server CD in the \support\debug\i386 directory.

You will need the following files to be put in your system directory:

dumpexam.exe

imagehlp.dll

kdextx86.dll.

It can be called as follows

dumpexam -v -f<output filename> <memory dump file>"

The -v flag indicates verbose output. The -f flag is used to specify the name of the text output file. If this flag is not used the output file will be memory.txt. The final command line argument is the name of the memory dump file. This is typically called memory.dmp and is contained in the windows system directory.

Common Errors

Install Shield -115 error

If NSM is uninstalled using add/remove programs or using the uninstall icon and then reinstalled without rebooting, the user might receive the Install Shield -115 error. The user must then wait for the system to cleanup and reboot the system before trying the install again. If this is not done the machine may be left in a state where NSM cannot be installed or uninstalled. In this case the user must do the following.

1. Click > Start > run and type "regedit"

2. Delete the following entries;

HKEY_LOCAL_MACHINE\SOFTWARE\IBM\IBM Network Station Manager

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IBM Network Station Manager

This is only known to happen with Lotus Go and not Microsoft IIS 4.

NSUpdate DOS window on Server

When DHCP is used for Network Stations a DOS window called NSUpdate will appear during reboot on the server. This window can be closed and will have no effect on NSM.

Netfinity Servers with multiple processors

At this time IBM DHCP cannot be installed on a Netfinity Server with multiple processors due to a driver conflict. When prompted to install IBM DHCP during install the customer must select "No". If "Yes" is selected the server could freeze after reboot. More information will be made available after further testing.

Korean Client Locale Settings

Currently Korean client users should select a different locale setting in NSM.. This will be corrected in an upcoming service update. The Korean server portion is functioning correctly.

Java Applet execution and Japanese/Korean locales

A code page problem inhibits java applet execution when the NT server is set to Japanese or Korean locales. This is a server code page issue and will be corrected in an upcoming service update. Please contact Development if a workaround is needed.

NSMUser and NSMAdmin Groups

In Release 3 and beyond the recommended NSM installation is on a Stand Alone Server or Stand Alone Server attached to a Domain. During NSM install the groups NSMUser and NSMAdmin are created on the NSM Server. All NSM users must be a member of the NSMUser group and administrators must be members of NSMUser and NSMAdmin. In order to log into NSM, domain users and administrators must be added to the local groups. These users can be added individually or in groups using Start\Programs\Administrative Tools (common)\User Manager for domains. The new users should be added and not recreated on the NSM Server. If there is the potential for multiple NSM Servers the users should be created on the domain to allow users and administrators login rights on multiple servers.

Network Station Login

This section contains tips for debugging network station login problems. When the IBM Network Station Login service encounters an error condition, it writes an entry to the Windows NT application event log. For each error, there are usually two entries. The first is NSL7015, which is a generic message that indicates that an error occurred. It is marked by a red icon in the event log. The second entry is an informational message that gives more details about the problem. It is marked by a blue icon in the event log. There are several types of informational messages. NSL7138 and NSL7139 occur during normal usage. NSL7138 means that the user could not be authenticated. It corresponds to the network station login panel message "User ID or Password is incorrect". NSL7139 means that the user's password has expired. It corresponds to the network station login panel message "Password has expired". The user will be prompted for a new password when this happens. Other event log entries usually do not occur under normal usage.

For each event log entry, here are some corrective actions to take:

NSL7138

The user name must exist on the machine where NSM is installed or on the Primary Domain Controller.

The user name and password must contain only invariant ASCII characters. The Installation and Use Guide lists the characters that are allowed in user names.

The user name must be in the NSMUser local group on the machine where the login service is installed.

The user's password must be correct.

The user must have the right to login in batch mode. They normally have this right because they are members of NSMUser, and we give the batch login right to NSMUser when we create the group at install time. To check this, go to User Manager->Policies->User Rights and check the Show Advanced User Rights check box. Then, make sure that NSMUser and NSMAdmin have the "Log on as a batch job" right. If these groups were created by the customer, rather than the NSM installation program, they will not have this right until it is manually added.

The user must not be outside of their allowed login hours. This property will only exist for users on a PDC. To check this, go to User Manager->User Properties->Hours. Make sure that the allowed login hours are correct.

NSL7139

This event log entry is made if the User Manager->Policies->Account->Maximum Password Age has been exceeded.

It is also made if the User Manager->User Properties->User Must Change Password At Next Login checkbox has been checked.

NSL7xxx

Other messages may indicate that there is a problem. If you feel that there is a problem, the following information will help development to investigate it.

Turn on login service logging and debugging. To do this, from Control Panel->Services, stop the login service. Next, type in -L -D in the Startup Parameters field. Then, restart the login service. This will write extra debug entries to the application event log for each login attempt. It should not be left on if the server is operating normally, since it will quickly fill up the log.

Save the system and application event logs. To do this, choose Event Viewer->Log->System, then Save As. Repeat with Event Viewer->Log->Application, then Save As.

Run the service tool as described earlier in this document.

Telnet into the client as described earlier in this document and capture an entire console trace from boot through login.

eNetwork on Demand

In addition to the NT event log used by all services, the following log files and tools are available in eNetwork on Demand. For more information please read the enod read.me.

DDNS server

SYSLOG file

The name server logs all significant events to the SYSLOG file, which is in OnDemand\Server\Etc\namedb directory. You can check the messages in this file to determine if there were problems in loading your configuration. The logging level and number of log files can be configured using the SYSLOG.CNF file or using the configuration program for the DDNS server. When the syslog file reaches the maximum size, it either wraps or is renamed to syslog.001, with syslog.001 being renamed to syslog.002, and so on, depending on how many files are being kept.

Two levels of logging are available: without debug-level messages (the default) and with debug-level messages. Usually the default is sufficient for normal usage. To enable the debug-level messages open the OnDemand\Server\Etc\namedb\syslog.cnf and remove the comment from the LOG_DEBUG entry.

NSUPDATE file

The NSUPDATE agent, used for an IBM DHCP server to perform DDNS updates, logs all significant events to the NSUPDATE.LOG file, which is in the OnDemand\Server\Etc directory.

The logging level and number of log files can be configured using the NSUPDATE.CNF file. When the nsupdate.log file reaches the maximum size, it either wraps or is renamed to nsupdate.001, with nsupdate.001 being renamed to nsupdate.002, and so on, depending on how many files are being kept.

Two levels of logging are available: without debug-level messages (the default) and with debug-level messages. Usually the default is sufficient for normal usage. To enable the debug-level messages open the OnDemand\Server\Etc\nsupdate.cnf and remove the comment from the LOG_DEBUG entry.

PING Command

To verify that the domain name server is working and can resolve names, use the PING command. The ping command sends an echo request to a remote host to determine if the host is accessible.

Syntax PING 'ip address'

PING Options

-d Starts the socket-level debugging process.

-r Bypasses the routing tables and sends packets directly to a host on an attached network. If the host is not on a directly-connected network, PING cannot make a connection. This parameter can be used to ping a local host through an interface that no longer has a route through it.

-v Specifies verbose output.

host Specifies the IP address or host name of the remote host to which you want to send the echo request.

data_size Sets the number of data bytes for the echo request (the default number of data bytes is 56, with an additional 8-byte header attached).

npackets Sets the number of echo requests that are sent to the remote host.

These parameters are position dependent; you cannot specify the number of packets without specifying the data size.

Note: If you do not specify npackets, the echo request is sent continuously until one of the following actions stops the echo request:

- Pressing the Ctrl and C keys simultaneously

- Pressing the Ctrl and Break keys simultaneously
- Closing the task

-? Displays help information.

DHCP Server

Defining DHCP log files

To enable logging by the server, all of the following must be specified in the OnDemand\Server\Etc\dhcpsd.cfg file.

- Name of DHCP log files
- Size of DHCP log files
- Number of DHCP log files
- At least one information type to log

Naming DHCP Log Files

Name the log file, using: **logFileName** *file_path*

The fully-qualified name that you assign to the current log file. The file name is a maximum of 8 characters. A file type is allowed for a DHCP log file. If no directory is specified, the default is the OnDemand\Server\Etc\ directory. If the specified path is not valid, the DHCP client continues to operate but does not log any information.

Defining the Size of DHCP Log Files

Specify the size of the log file, using: **logFileSize** *value*

The maximum log file size in kilobytes. The minimum size is 1KB.

Defining the Number of DHCP Log Files

Specify the number of log files maintained, using: **numLogFiles** *value*

The maximum number of log files maintained.

Notes:

If the value for numLogFiles is 0 or the statement is omitted, no logging occurs.

If a new log file is created after the maximum number is reached, the oldest log file is removed.

The maximum number of files is specified by the file system. For example, 999 files is the maximum value on a FAT file system.

If the value for numLogFiles is greater than 1, when the size of the most current log file reaches the maximum size, it is renamed by removing the initial filetype of LOG and appending an integer as the filetype to the log file name. A new log file is created as the current log. All older files are renamed by incrementing the previously appended integer filetype by 1. The larger the file type extension, the older the log file. For example, DHCPLOG.003 is an older log file than DHCPLOG.001.

Specifying Information Types to Log

Specify information types to log, using: **logItem** *type*

Types include:

SYSERR Errors at the interface to the operating system

OBJERR Errors between objects in the process

PROTERR Protocol errors between the client and server

WARNING Warnings that warrant the user's attention

EVENT Events in the process

ACTION Actions taken by the process

INFO Useful information

ACNTING Accounting information, such as who was served

TRACE Trace information

STAT Statistics at each DHCP database update interval

IBM Intermediate Support Driver

To help identify problems, you can start and stop a trace while the IBM Intermediate Support Driver is running. That is, you can turn tracing on and off without stopping the driver.

The trace data is written in binary format and the output file is "path\wejtrace.n". The path and file name, as well as other parameters, can be specified when the trace is started. The default path is the directory from which the trace is being run. n is 1 or 2. It is intended to be read by IBM Service only, so a trace viewer is not installed on the server. The trace can be collected continuously in bounded files so that it can be left running without consuming large amounts of disk space.

To collect trace data, use the wejtrcol program from a command prompt. You can also type wejtrcol -? for options.

NFS server

NFS Trace configuration

Enable trace

The Enable trace field determines whether the NFS server will write the trace information to the etc\nfsdtrce.trc file. When checked, the trace records are written to the trace file. You can turn tracing on and off while the NFS server remains active. When tracing is turned on, the NFS server opens the trace file for writing trace information and leaves it open until tracing is turned off or until the Trace file name is updated. The NFS server closes the trace file either when tracing is turned off, or the NFS server stops, or the Trace file name is changed.

Trace file name

The Trace file name is the fully qualified path name which identifies the file that stores the trace records. To start the NFS server tracing, check the enable trace field. The default Trace file name is nfsdtrce.trc and it is in the \ETC directory, relative to the product installation path. You can select the trace information that you want to record. When tracing is started, all contents of the trace file will be discarded. To use another file name, type the file name or click Browse to select the path and file name. The maximum length of the Trace file name is 256 characters. If you use a longer file name, it will be ignored and the default file name is used. If you use a relative path or do not specify the path, the file will be created in the %systemroot%\system32 directory. Before you change the Trace file name, make sure you check Enable trace. To record trace information from the NFS server, provide write access to the path and trace file, and the file must not be a read-only file. An error will be logged to the Event Log if the NFS server cannot open the trace file, and no tracing will occur. No error will be logged if the NFS server can open a trace file but cannot write an individual trace record.

To erase the trace file, first stop the trace so that the NFS server will close the file.

Trace options

You can selectively record only some of the trace information. To choose the trace options:

Make sure enable trace is checked.

Select the level of trace information:

- Minimum trace
- Intermediate trace

- Maximum trace

    Click File, then Save to save your changes.

Time server

The output file for Time Server tracing is etc\timed.log.

The trace information includes the time sent to a client, system calls, and return codes. It is intended for IBM service personnel only. You will not need to view or use the contents of the trace file. The trace information is recorded in plain text and in U.S. English only, so it can be viewed with Notepad.

To help identify problems, you can start and stop a trace.

Click Start > Programs > eNetwork On-Demand Server > Time Server Configuration.

Click the Trace tab.

The trace information is written to the file specified in the trace name field.

Click the enable trace checkbox so that it is checked.

To stop tracing, click the enable trace checkbox so that it is unchecked.

Click File > Save to save your changes.

Changing to another trace

You may want the trace information in a separate file. To change to another trace file:

Click Start > Programs > eNetwork On-Demand Server > Time Server Configuration.

Click the Trace tab.

Make sure enable trace is checked.

Change the trace file name to another file name. A common convention is to number the trace files, such as timed2.log.

Click File > Save to save your changes.

The trace information will be recorded in the file you just named.