Network Traffic Management

8920 Network Traffic Management software

System Administration Guide
Release 17.3

190-406-814
Issue 1.0
October 2012

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Trademarks

All trademarks and service marks specified herein are owned by their respective companies.

Warranty

Alcatel-Lucent provides a limited warranty to this product.

Customer Notification

The Alcatel-Lucent contract specifies your system configuration (e.g., capacities) and identifies the optional features you have purchased.
The standard NTM Feature Set documentation contains information on all of the features available in the Release, including those you may not have purchased, which are thereby not available for use.
Alcatel-Lucent will not support external use of the third-party software packages included in the NTM Feature Set.

Acknowledgements

We wish to acknowledge:

ACP50 and ACP550 are products of NetKit Solutions LLC.

The NTM product includes software developed by:

Red Hat Enterprise Linux® - Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

APACHE TOMCAT - The Apache License, version 2.0 (http://www.apache.org/licenses/).

APACHE ActiveMQ - The Apache License, version 2.0 (http://www.apache.org/licenses/).

MOD AJP (APACHE Tomcat Connectors) - The Apache License, version 2.0 (http://www.apache.org/licenses/).

Apache Xerces C++ - The Apache License, version 2.0 (http://www.apache.org/licenses/).

Apache Axis2 - The Apache License, version 2.0 (http://www.apache.org/licenses/).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MOD_SSL - Copyright (c) 1998-2004 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bugzilla - Mozilla Foundation; License: http://creativecommons.org/licenses/by-sa/2.0/

CentOS - CentOS Project;

Dom4J - DOM4J Project; License: http://www.dom4j.org/dom4j-1.6.1/license.html

LDAP C SDK - Mozilla Foundation; License: http://www.mozilla.org/MPL/MPL-1.1.html

mksh - Korn shell by David Korn; Distributed under BSD License. (https://www.mirbsd.org/htman/i386/man7/BSD-Licence.htm)

ncurses - ncurses, GNU 5.5; Distributed under MIT + GPL2+

nmon - IBM nmon; License: http://www.gnu.org/copyleft/gpl.html

PAM_RADIUS_AUTH - This module is a merger of an old version of pam_radius.c, and code which went into

mod_auth_radius.c, with further modifications by Alan DeKok of CRYPTOCard Inc.. The original pam_radius.c code is copyright (c) Cristian Gafton, 1996, redhat.com> The additional code is copyright (c) CRYPTOCard Inc, 1998. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU Public License, in which case the provisions of the GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential bad interaction between the GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JAVA JDK - Sun Microsystems Inc. Binary Code License Agreement (http://java.sun.com/j2se/1.5.0/jdk-1_5_0_12-license.txt).

edtFTPj - Enterprise Distributed Technologies under LGPL License (http://www.gnu.org/licenses/lgpl.txt).

Perl DBD - Perl DBD Copyright (c) 1994-2003 Tim Bunce, Ireland is used with permission. Distributions of the standard package can be found through the http://www.cpan.org website.

Perl Convert::ASN1 - Perl DBD Copyright (c) 1994-2003 Tim Bunce, Ireland is used with permission. Distributions of the standard package can be found through the http://www.cpan.org website.

Perl URI - Perl DBD Copyright (c) 1994-2003 Tim Bunce, Ireland is used with permission. Distributions of the standard package can be found through the http://www.cpan.org website.

Prototype - Copyright (c) 2005-2007 Sam Stephenson

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Scmbug - Scmbug by Martin Tomes; License: http://www.subversionary.org/projects/scmbug

SNMP4j - SNMP4J.org; License: http://www.snmp4j.org/LICENSE-2_0.txt

Subversion - CollabNet; License: http://subversion.tigris.org/license-1.html

SWISH-E - Copyright 1995-1998 by Miles O'Neal, Austin, TX, USA. GNU General Public License.

w4ais - Copyright 1995-1998 by Miles O'Neal, Austin, TX, USA. (http://yolo.net/w4ais/license.html)

GNU LESSER GENERAL PUBLIC LICENSE - Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to ecompile the application to use the modified definitions.)

b) Use a suitble shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

JSch 0.0.* was released under the GNU LGPL license. Later, we have switched over to a BSD-style license.

Copyright (c) 2002-2010 Atsuhiko Yamanaka, JCraft,Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JCRAFT, INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Contents

5 Backing Up and Restoring the System

6 Generating a Crash Dump

7 Administrative Performance Reports

8 Database Administration

9 Adding and Removing Network Elements

10 Time Synchronization

11 Subnetwork Administration

12 BDR Administration on a Host

16 UDDM/UDNEI Administration

17 *Navis* Identity Software

List of figures

1 Overview of System Administration

2 Adding and Removing Users on the Host

3 System Security, User Groups, and Group Permissions

4 Starting and Stopping the System

5 Backing Up and Restoring the System

6 Generating a Crash Dump

7 Administrative Performance Reports

List of tables

1 Overview of System Administration

Overview

Purpose

This guide provides administration procedures and reference information needed to administer the 8920 Network Traffic Management software.

Installation-related procedures

For the sequence of tasks located in this guide that are needed as part of the 8920 NTM installation, see "High-level process required to install NTM" (p. 10) in the *Installation Guide*.

Contents

This chapter contains the following topics:

□

Chapter organization

Administration tasks

Administration tasks are those that are performed by the system administrator, including:

- Chapter 2, “Adding and Removing Users on the Host”
- Chapter 3, “System Security, User Groups, and Group Permissions”
- Chapter 4, “Starting and Stopping the System”
- Chapter 5, “Backing Up and Restoring the System”
- Chapter 6, “Generating a Crash Dump”
- Chapter 7, “Administrative Performance Reports”
- Chapter 8, “Database Administration”
- Chapter 9, “Adding and Removing Network Elements”
- Chapter 10, “Time Synchronization”
- Chapter 11, “Subnetwork Administration”

Tasks related to purchasable features

This guide also includes information on administering the various purchasable features available with NTM, including:

- Chapter 12, “BDR Administration on a Host”
- Chapter 13, “ARC Administration”
- Chapter 14, “Capacity and Usage Reporting”
- Chapter 15, “Surveillance Transition to Additional Trunk Groups”
- Chapter 16, “UDDM/UDNEI Administration”

Report Writer feature

Some functions found in this guide can also be performed on a coresident or stand-alone Report Writer host. These chapters contain procedures that are valid for Report Writer systems:

- Chapter 2, “Adding and Removing Users on the Host”
- Chapter 4, “Starting and Stopping the System”
- Chapter 5, “Backing Up and Restoring the System”
- Chapter 6, “Generating a Crash Dump”

□

Helpful tips

Auto terminate shell

To auto terminate the shell after a specified period of inactivity on the terminal, the user can set the shell parameter TMOUT.

Its value can be set:

- in the *"/etc/profile"* file in which case it will be applicable to all users
- in the *".profile"* file of individual users
- at the command line

Example:
TMOUT=300
export TMOUT

The shell terminates if no command is entered within 300 seconds (+ 60 seconds grace period) after the PS1 prompt has been issued.

The su command

The `su` command is used to change from your original login permissions to superuser permissions. The `su` command logs each attempt to become superuser in the *"/var/adm/sulog"* file. The entries in the file look like the following:

```
SU 04/04 12:45 - ttyp2 mff-nmadm
SU 04/04 12:45 + ttyp2 mff-nmadm
SU 04/04 13:00 + tty?? root-adm
SU 04/04 14:00 + tty?? root-adm
SU 04/04 14:25 + ttypc jss-root
SU 04/04 14:40 + 16 nmadm-root
SU 04/04 14:41 - ttypc jll-root
SU 04/04 14:41 + ttypc jll-root
SU 04/04 15:00 + tty?? root-adm
SU 04/04 16:00 + tty?? root-adm
SU 04/04 17:00 + tty?? root-adm
```

The *"/var/adm/sulog"* file also contains log entries for system events such as unsuccessful su attempts. When the file gets too large it is moved to *"/var/adm/OLDsulog"*. The new logs are then contained in the *"/var/adm/sulog"* file.

The lock command

The `lock` command is used to lock a terminal. It requests a "key" from the user, confirms it, and then prints LOCKED on the terminal. It then refuses to relinquish the terminal until the key is entered. The user can unlock the terminal by entering the `"key"` again. If the user forgets the password, the user must log in elsewhere and kill the lock process or turn the terminal off, then on, and login again.

The last command

The `last` command is used to get information on all of the successful logins and logouts on the system. It searches backwards through the file *"/var/adm/wtmp"* for information about a user, a tty, or any group of users and ttys. It prints the sessions of the specified users and ttys, most recent first, indicating when the session began, the duration of the session, and the tty on which the session took place. It also indicates if the session is still in progress or if it was cut short by a reboot. This works with login attempts through telnet and rlogin.

The lastb command

The `lastb` command can be used to get information on all of the unsuccessful logins on the system (i.e. any instance of login attempt without giving a valid password). It searches backwards through the file *"/var/adm/btmp"* (bad login database file) to display unsuccessful login information. This works with login attempts through telnet and rlogin.

The dmesg command

The `dmesg` command can be used to view system diagnostic messages. It looks in a system buffer for recently printed diagnostic messages and prints them on the standard output. The messages are those printed by the system when unusual events occur, such as: when system tables overflow, system detects hardware errors, or the system crashes.

The top command

The `top` command can displays the top processes on the system and periodically updates the information. Raw CPU percentage is used to ranks the processes. To exit the program and resume normal activities, type `"q"` at any time. Top can be executed with or without command line options. Read the man page on the `top` command for more information.

□

Troubleshooting recommendations

Powering off

Never power off the disk array, unless told to do so by NTM customer support.

- Power cycling the disk array increases the likelihood of premature failure, especially if the disk array has not been power-cycled for a long time.
- Data could be lost if there are faults with the cache.
- The disk array is a high availability device. Powering it off defeats the purpose of having a high availability device on the system.

Hardware swapping

- Never remove or swap hardware with the power off.
  - Remove faulty or suspect hardware, or install new hardware, with the power ON. The disk array must know the state of the hardware and its configuration to be able to keep the database disks up to date.
- Never swap suspect hardware between disk arrays.
  - Always use original replacement parts to replace suspect hardware. Swapping parts between a faulty disk array and a working disk array can result in two faulty disk arrays.

□

2 Adding and Removing Users on the Host

Overview

Purpose

This chapter describes how to add and remove users from the host processor using the `addntmuser` and `delntmuser` commands, respectively.

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Adding users" (p. 4)	5 minutes	X	X
"Removing users" (p. 5)	5 minutes	X	X

Contents

This chapter contains the following topics:

□

Process: Adding and removing users

Purpose

The addntmuser and delntmuser commands adds or removes RDB credentials.

Important! Users must be added or removed both in the relational database (RDB) and in the browser-based GUI environment to have full application access. To add users in the GUI environment, see "Adding users" (p. 55) in the User Guide . To remove users from the browser-based GUI environment, see "Deleting users" (p. 57) in the User Guide .

Note, prior versions of 8920 NTM used the command names adduser and deluser, these names were in conflict with commands supplied by the Linux OS, hence the NTM command name change to addntmuser and delntmuser. Please be sure to use the new command names when managing NTM users. Also, the NTM product is not constructed for operation using SE (Security Enhanced) Linux or Access Control Lists (ACLs).

addntmuser

Use the addntmuser command to add new users to the NTM application relational database (RDB).

delntmuser

Use the delntmuser command to remove users from the NTM application relational database (RDB).

□

Adding users

Instructions

Follow these steps to add users:

1 Coordinate with your System Administrator to create the needed new user and/or groups at the Operating System (OS) level. The method used here for OS level user and group management is site dependent.

2 After the user has been created at the OS level login as the nmadm user at the command line.

3 To give this new user NTM application data access the user must be added to the relational database (RDB), this is accomplished using the addntmuser command. You may add the new username by supplying it as a command line argument or be prompted for the username if no argument is given.

Example:

```
addntmuser <username>
```

or

```
addntmuser
```

4 Once the user's NTM RDB credentials have been added this user may be utilized for Web GUI data access. See the Web User administration section of the User Guide for details.

END OF STEPS

□

Removing users

Instructions

Follow these steps to remove users:

1 To remove the user from Web GUI access see the Web User administration section of the User Guide.

2 Become the `nmadm` user at the command line.

3 Remove the user from the relational database (RDB) using the delntmuser command. You may remove the username by supplying it as a command line argument or be prompted for the username if no argument is given.

Example:

```
delntmuser <username>
```

or

```
delntmuser
```

4 Coordinate with your System Administrator to remove the user and/or groups at the Operating System (OS) level. The method used here for OS level user and group management is site dependent.

END OF STEPS

□

3 System Security, User Groups, and Group Permissions

Overview

Purpose

This chapter discusses system security and creating and removing user groups. By controlling the user groups, you can allow or refuse access to system commands and files.

> **Important!** You must have `superuser` permission to complete some of the processes in this chapter.
>
> **Reference:** "The su command" (p. 4)

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	**Approximate Time Required**	NTM **Host**	**Report Writer Host**
"Using the snw_admin command to add user groups" (p. 20)	5 minutes	X	

Procedure	Approximate Time Required	NTM **Host**	Report Writer Host
"Removing user groups" (p. 23)	5 minutes	X	
"System Notices" (p. 13)	15 minutes	X	

Contents

This chapter contains the following topics:

□

Predefined valid user groups

Overview

The following is a list of the predefined valid user groups to be created for proper NTM application operation. These groups are to be created before NTM application installation.

> **Important!** These groups should not be removed or modified after installation. Other groups, however, may be added.

- System Administrator group (`sys`) — This group has permission to execute application shell programs, as well as any command or page for any and all subnetworks in the system.
- Super network manager group (`snm`) — This group has permission to execute any command or page for any and all subnetworks in the system.
- Super record base group (`srb`) -- This group has permission to execute any command targeted for the " rb " group for any and all subnetworks. Do not place this group in the "/nm/etc/permissions" file.
- Network manager group (`nm`) — This group has permission to run controls, view data, and interact with network offices in any manner.
- Record base group (`rb`) — This group has permission to insert, modify, or delete information from the record base and run the `create` and `installdb` commands.
- Browser group (`nsgroup`) — This group has permission to change browser server information and preferences.
- Oracle install group (`oinstall`) – This group is associated with the oracle user and group ownership of the install Oracle Relational Database.
- WebGUI users group (`ntmgui`) - This group is an optional default user group to allow for proper NTM Web GUI operation. This group appears in the default NTM installations as a convenience. For proper NTM Web GUI operation the Host UID user(s) associated with the Web GUI must be a member of at least one of the groups appearing in the */etc/suders.d/ntm-50-nsadmin-gui* file. The sudoers entry in this file lists the user groups that will operate properly within the NTM Web GUI. The default NTM installation includes groups, `nm`,`snm`, and `ntmgui`. This entry should not be changed but may be extended by adding other user groups.

References

"installdb" (p. 34) in the *Input Commands Guide*

□

Predefined user logins

Overview

The following is a list of the predefined valid users to be created for proper NTM application operation. These users are to be created before NTM application installation.

Important! These logins should not be removed or modified. Other logins, however, may be added.

- NM Administrative login (`nmadm`).
- Browser Administrator (`nsadmin`).
- Oracle Relational Database login (`oracle`).
- OSTC Support login (`ostc`) - NOTE: The ostc user is not strictly required for proper NTM application operation. The ostc user is the traditional NTM product support id and may be substituted with a different id name if necessary, but retain the group membership listed. Failure to provide a support account can substantially complicate and delay resolution of support items.
- Default Web GUI Administrator login (`netadmin`) – NOTE: upon initial install the default Web GUI password for the `netadmin` user is netadmin. This password should be changed upon completion of installation.

Table

Table 1 provides the initial login group setting for each user and their required group membership.

Table 1 Initial login group setting for each user and their required group membership

User Name	Initial Login Group	User Group Membership
`nmadm`	`snm`	snm, nm, rb, dba, sys, srb
`oracle`	`oinstall`	oinstall, dba
`nsadmin`	`nsgroup`	nsgroup
`ostc`	`snm`	snm

□

NMADM login accountability

Overview

Feature 22, “NMADM Login Accountability” increases the level of security in the NTM system without restricting user activity. This feature allows the administrator to

- eliminate the usage of the nmadm group login
- log the usage of application commands and pages

Important! Feature 22, “NMADM Login Accountability” (NMLOG) is optional. It is available only if it has been purchased.

With this feature, it is no longer necessary to use the `nmadm` password to stop and start the system. Everyone in the snm user group automatically has permission to run any of the nmadm commands (`bdr_act`, `startsys`, `stopsys`, `limitthr`, and `recreate`) without a password. The administrator has the option of allowing an entry to be made in the command log file (*“/musr/log/cmdlog”*) each time any of these commands, or any command or page in the permissions file, is executed.

Figure

Figure 1 shows an example of the format of the *“/musr/log/cmdlog”* file.

Figure 1 Format of the “/musr/log/cmdlog” file

```
# date/time        user-id  message    command command args
#
00/12/01-15:34       nmadm PERMISSION  act stbdcp1
00/12/01-15:50     jsigler PERMISSION  recreate
00/12/01-15:52       nmadm PERMISSION  cant
00/12/01-15:54       nmadm PERMISSION  dbtest files=office office=5e15+noxfer
00/12/01-15:54       nmadm PERMISSION  deact 5e15
00/12/01-15:55       nmadm PERMISSION  act 5e15 audit
```

Logging commands

The administrator determines which commands to log by modifying the log field in the *“/nm/etc/permissions”* file.

When the command log file (*“/musr/log/cmdlog”*) reaches a certain size, the system automatically copies it to the file *“/musr/log/cmdlog.old”*. When this happens, any old information stored in *“cmdlog.old”* is overwritten.

System security

The overall security of the system remains the responsibility of the system administrator. The `root` login can override usefulness of Feature 22, “NMADM Login Accountability” and therefore its access should be closely monitored and limited.

Important! When Feature 22, “NMADM Login Accountability”, and Feature 8, “Disaster Recovery (Duplex)” and Feature 40, “Enhanced Disaster Recovery” are installed, certain commands are logged in the cmdlog file on both the primary and backup hosts. If a non-standard security system is installed, the command log may not report the same user ID on the backup host as it does on the primary host.

□

Permissions file

Overview

NTM supplies a permissions file to determine which user groups are permitted access to the NTM commands and pages. System security is maintained through the following types of permissions:

- *Linux* operating system file permissions (user groups and logins)
- Application administrator-definable set of permissions (permissions file)
- Subnetwork permissions

Definition

The permissions file:

- is an ASCII file maintained by the system administrator
- consists of a list of NTM application actions in the system, a logging option, and the user group names that can execute them
- is used by the system administrator to define which user groups are permitted to run the NTM commands and pages, and, if Feature 22, "NMADM Login Accountability" has been purchased, which commands and page executions are to be logged.

NTM components affected

The set of permissions defined by the system administrator affects only the NTM commands and pages. Through the NTM permissions file, you can customize your system to restrict access to commands to certain groups of users.

> **Important!** To execute some commands, such as `startsys` and `stopsys`, the user must know the `nmadm` password in addition to having the group ID in the permissions file. If Feature 22, "NMADM Login Accountability" has been purchased, the `nmadm` password is not used.

Group-based

Permissions in NTM are group-based, not login-based. This means that all members of a group have command permissions defined for that group in the permissions file.

Changing permissions

The system administrator initially defines and can subsequently change the command permissions. User group permissions are defined in the *"/nm/etc/permissions"* file.

References

Chapter 11, “Subnetwork Administration”;

Permissions file layout

Fields

The permissions file is divided into five fields:

- An `executable` field (also referred to as command field)
- A `field separator` (by default, a single pipe character [|])
- A `log` field (“l” for logging and “n” for no logging)
- A second `field separator` (by default, a single pipe character [|])
- A `group name` field that defines the user group (or groups) allowed to run the command

Comments

You can place comments into the file if they are preceded by a pound sign (#) and remain on a separate line within the file. Do not place comments at the end of a valid group list or anywhere within a permission record.

Figure

Figure 2 shows an example of a permissions file.

Figure 2 Permissions file

```
#COMMENT LINE,   SHOULD BE IGNORED
#COMMAND LOG?    VALID GROUP LIST
#-------------------------------
cg       |l|     nm
canf     |l|     nm
cant     |l|     nm
skip     |l|     nm
audit    |l|     nm rb usr
ctrlog   |n|     nm usr
ocldtn     |l| nm
oclendpnt  |l| nm
oclrealm   |l| nm
ratelimit  |l| nm
ratelimitpolicy |l| nm
EXEC     |l|     nm
EXECBG   |l|     nm
VALID    |n|     nm
```

□

Editing the permissions file

Text editors

You can edit the permissions file by using any *Linux* system text editor. However it is strongly recomended to use viperm command to edit permissions file in a safe way.

For more information how to use `viperm` command and check the syntax of the permissions file, see Chapter 7, “viperm” in the *Input Commands Guide*.

Syntax

Use the following format to add entries to the file:

```
command | log | [[grp1] [grp2] ...] ;
```

Parameters

`command` is the name of the NTM command or shell script for which you want to specify permissions

`log` specifies whether logging is turned on (**l**) or not (**n**) for the command

> **Important!** The logging option is part of Feature 22, “NMADM Login Accountability” and is available only if the feature has been purchased.

`[grp1] [grp2] ...` are the NTM group name(s) allowed to execute a specified command. You can list a maximum of 30 unique groups.

Group names

The *`command`* name is required, but the `group names` are optional. If you do not specify an entry or specify a hyphen (`-`) in the `group names` field for a particular page, command or shell script, only the users of the “`snm`” group have permission to execute the command. If you have purchased Feature 22, “NMADM Login Accountability” and you specify “`sys`” in the `group name` field, the `root` login will have permission to execute the command.

> **Important!** Do not remove the “`sys`” group entry for any commands in the default permissions file. However, you may add the “`sys`” group entry for any other commands. Save a copy of the default permissions file before performing any edits.

Commands names

If a command name is not included in the permissions file, anyone can use the command, provided they have the appropriate *Linux* system and subnetwork permissions.

□

Password Administration

Overview

There are two types of passwords associated with NTM application: those for the Command Line Interface (CLI) and those for the Web Graphical User Interface (GUI). The administration of these passwords generally involves configuring password complexity, aging, locking, etc.

Administration of the passwords for the CLI interface depends on the authentication modules used. The user is directed to the appropriate Pluggable Authentication Module (PAM) for information on how to administer the various aspects of CLI passwords.

Web GUI password administration relies on the use of the standard PWA feature available to all customers and/or the EPWA purchasable feature. The description of these features' use and configuration is defined in the *User Guide* under the GUI Administration chapter.

> **Important!** At initial system turn-up, a default Web GUI user is installed with administration permissions. The user id is `netadmin` with password netadmin. The user or installation personnel should change the `netadmin` password upon completion of NTM application installation.

□

System Notices

Overview

Purpose

There are a number of notices (or banners) that may be configured and displayed to users. The usual purpose of these notices is to announce to users that system access is restricted to authorized individuals and to indicate the legal ramifications of system use; thereby mitigating an intruder's argument that they were unaware of the consequences related to its improper use.

On a host running the NTM application there are generally two interfaces the user will encounter:

1. The Command Line Interface (CLI)
2. The Web Graphical User Interface (GUI).

Notices associated with the CLI are generally governed by capabilities provided by the host Operating System (OS) and its installed applications. The NTM Web GUI provides a means to configure a notice displayed to Web users upon initial system access via a browser session.

Contents

This section contains the following topics:

□

Configuring CLI Notices

Purpose

Due to the array of authentication and 3rd party application modules available, not all possible conditions of notice specification can be defined. However, the "base" configuration of a newly installed NTM system has certain areas in which a customized notice can be presented to users. If you want to use a specific authentication module or 3rd party application, then the documentation for that software must be consulted for methods of supplying notices.

Following are the general areas for which CLI notices may be specified:

- The first place a notice can be added is in the */etc/motd* (message of the day) file. This file's contents are often displayed to the user regardless of access mechanism (ssh, telnet, rlogin, etc). Note: NTM provides a default file that will be displayed (*/nm/etc/rnms.motd*) if the event */etc/motd* is not present.
- For ssh, scp, and sftp, edit the */etc/ssh/sshd_config* file and search for the text "`Banner`". If found, uncomment the entry (if required) and set its argument to point to a text file containing the desired notice text. If "`Banner`" is already found in the file, simply insert a new "`Banner`" line. Be sure to use a fully qualified name for the path to the file containing the notice text. To cause the sshd daemon to immediately pick up this Banner file you must become the root user and perform a "`kill -SIGHUP <sshd pid>`"; otherwise, the notice will be picked up upon the next system reboot. Please see the manual page for `sshd_config` and `sshd` to ensure proper configuration.
- As initially installed, the NTM host will not have the telnet daemon enabled for security reasons. Instead, ssh should be used and is enabled by default. However, if an administrator decides to enable the telnet daemon, a notice can be displayed during login by placing the notice text in the */etc/issue.net* file.
- A notice message can be created for console login by editing the */etc/issue* file. Note: both the *issue* and *issue.net* files support certain escape/character sequences to allow dynamic insertion of some information. Please see associated manual pages and documentation for specifics.

Instructions

To configure the text for the login dialog perform the following:

1 Coordinate the following change with the NTM users, as this procedure will cause a brief interruption in Web GUI access.

2 Login as `root`.

3 Eexecute: `cd /nm/web/sup_soft/http/conf`

4 Allow restoral of the Web server configuration should an error occur by executing: `cp httpd.conf <to a backup name>`

5 Edit the *httpd.conf* file and search for the text “`AuthName`”.

6 Change the text in quotes beside the “`AuthName`” parameter to the desired text. Try to limit the text length to 80 characters if possible.

7 Test your changes with a representative browser to ensure they appear correctly once you have restarted the server. As delivered, the dialog text is set to “NTM”.

8 Write the file and exit.

9 Go to directory: `cd /nm/web/sup_soft/http/bin`

10 Restart the Web server by executing: `./reload-server`

Result: If the server restarted successfully you will see an “`Ok`” message. If there is a failure, verify your change or replace the *httpd.conf* file with the one saved in Step 4 and execute `./reload-server` again to restore Web GUI functionality.

END OF STEPS

□

Configuring GUI Notices

Purpose

The Web GUI has the ability to display user configurable text in the login dialog box during Web GUI authentication. However, due to the varying capabilities of different Web browsers and versions of web browsers, using this as the sole means of providing necessary notice text may not be sufficient. In addition to text in the login dialog, you can configure a notice to be displayed and acknowledged at the start of each new browser session.

Instructions

To configure the Web GUI notice text use the following procedure:

1 Edit the */nm/etc/rnms.motd* file and insert your notice.

2 In order to add visual components into the notice, use the */nm/etc/motd.html* file. The html version dynamically includes the */nm/etc/rnms.motd* content and allows defining a logo, borders, styles, etc. For example:

```
<html>
<style>
   /* customer can add style here */
</style>
<body>
    <img src="logo.png" alt="customer's logo" />
    <div class="MOTD">
        { /nm/etc/motd file content is dynamically included
  here }
    </div>
</body>
</html>
```

END OF STEPS

□

Display Managers

Overview

If an X display manager, such as the GNOME display manager, is used, you may wish to construct notice text for this GUI interface as well. The GNOME display manager (GDM) is the default one supplied with Red Hat; however, there may indeed be other display managers present. Please consult your display manager documentation for instructions on modifying the login notice/greeting.

□

Adding and removing user groups

Overview

Purpose

A user group determines a person's subnetwork and command permissions in NTM. Therefore, it is important to create user groups with the desired permissions.

This section also provides information about removing user groups using the `snw_admin` command.

Contents

This section contains the following topics:

□

Using the snw_admin command to add user groups

Purpose

The `snw_admin` command is a page-like command primarily used to set up and administer subnetworks.

Upon entering the `snw_admin` command, you will see the main subnetwork administration menu.

After choosing the `add user group` option from this menu, you are prompted for

- the name of the user group
- the home subnetwork
- the user group permissions

Instructions

Follow these steps to add user groups using the `snw_admin` command.

1 Log in as `nmadm` or some other user in the snm group.

2 Enter `snw_admin`.

Result: The system displays the Subnetwork Administration menu (Figure 3, “Subnetwork Administration menu” (p. 22)).

3 Enter `3` to select the `add user group` option.

4 Enter the name of the user group you want to add.

Hint: The group you are going to add must exist in the system.

5 Enter the home subnetwork of the user group.

Important! Although permissions can be changed, you should assign user groups to the subnetworks they usually manage.

6 Enter `YES` to add the user group.

7 Set Subnetwork Permissions with one of the following.

- Enter `1` to set the default permissions of surveillance, control, and audit permissions for the user group's home subnetwork.
- Enter `2` to set no subnetwork permissions.
- Enter `3` to enter subnetwork permissions other than the default.

Notes:

- If you set no permissions, the group will not be able to access any office or trunk group information.
- If you set permissions other than the default, ***SAVE*** those permissions before you continue.

8 Set the database modification permissions (if applicable) with one of the following.

- Enter `1` to set no database modification permissions.
- Enter `2` to enter database modification permissions.

Important! You need only enter database modification permissions if you have purchased and are using Feature 3, "Management of Record Base Partitions and Subnetworks".

If you enter database modification permissions, save them before continuing with the next step.

Reference: "Database modification permissions" (p. 5)

9 Set the command permissions with one of the following.

- Enter `1` to assign no command permissions.
- Enter `2` to assign the same command permissions as another user group.

Notes:

- If you pressed `2` then enter the name of the group whose permissions you want to have for this user group. Enter `y` to save the permissions.
- If you prefer to enter permissions directly in the *"/nm/etc/permissions"* file, choose to set no permission in the `snw_admin` menu and then edit the *"/nm/etc/permissions"* file later.

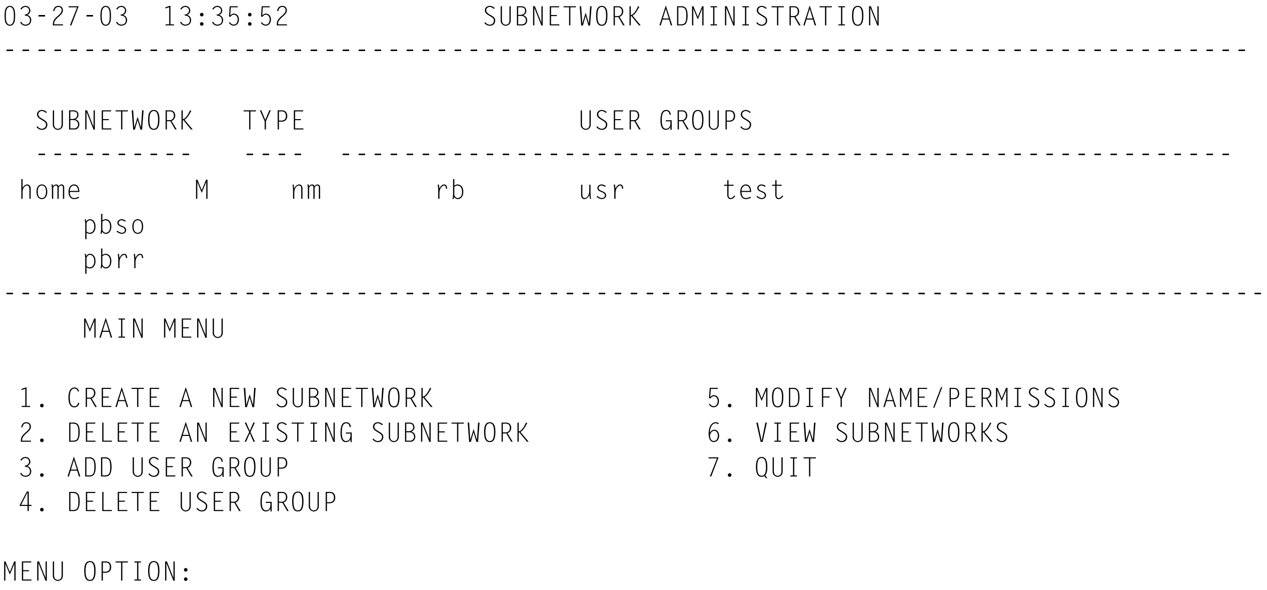
10 Enter 1 to return to the subnetwork administration main menu and then press 7 to quit from the menu.

END OF STEPS

Figure

Figure 3 shows the subnetwork administration menu.

Figure 3 Subnetwork Administration menu



```
03-27-03  13:35:52            SUBNETWORK ADMINISTRATION
-------------------------------------------------------------------------------

  SUBNETWORK   TYPE                  USER GROUPS
  ----------   ----  --------------------------------------------------------
 home        M     nm        rb        usr       test
     pbso
     pbrr
--------------------------------------------------------------------------------
     MAIN MENU

 1. CREATE A NEW SUBNETWORK                    5. MODIFY NAME/PERMISSIONS
 2. DELETE AN EXISTING SUBNETWORK              6. VIEW SUBNETWORKS
 3. ADD USER GROUP                             7. QUIT
 4. DELETE USER GROUP

MENU OPTION:
```

□

Removing user groups

Instructions

Follow these steps to remove user groups using the `snw_admin` command.

1 Log in as `nmadm` or another user in the snm group.

2 Enter `snw_admin`.

Result: The Subnetwork Administration menu appears (Figure 3, "Subnetwork Administration menu" (p. 22)).

3 Select the `delete user group` option.

4 Enter the name of the user group you want to delete.

5 Press `Y` to delete the user group.

Result: At this point, the user group has been removed from NTM memory and all subnetwork and command permissions for that group have been removed. However, the user group still exists in the system.

6 Press `1` to return to the subnetwork administration menu.

7 Press `7` to exit from the subnetwork administration menu.

8 Use `delntmuser` to remove user's RDB credentials. When finished reassign each user of this group to a different group in the system.

9 Use the `chgrp` (change group) command to change any files that have in their inode structure the group ID of the group to be deleted.

10 Log in as `root` and remove the group you deleted in the subnetwork administration menu from the *system*.

Result: The user group is now completely removed from the system.

END OF STEPS

References

See the host documentation for more information on the *Linux* operating system `chgrp` command.

□

4 Starting and Stopping the System

Overview

Purpose

This chapter discusses how to start/stop and halt/boot the NTM system and the map data server. The process of starting NTM initiates many of the low-level processes that occur every day. These processes include:

- exception processing
- data collection
- the database servers
- the audit server
- CC (Configurable Converter)
- HOD (Host Oracle Dumper)

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Starting the NTM application" (p. 4)	5 minutes	X	
"Stopping the NTM application" (p. 5)	5 minutes	X	
"Starting the map data server" (p. 8)	5 minutes	X	
"Stopping the map data server" (p. 9)	5 minutes	X	
"Normal halting and booting procedures" (p. 13)	30 minutes	X	

Contents

This chapter contains the following topics:

□

Starting and stopping the NTM system

Overview

Purpose

The process of stopping NTM gracefully shuts down these low-level processes. Shutting down the system enables you to:

- Back up, reload the current database
- Install a new database
- Respond to system error messages
- Reboot the processor

Important! To reduce database corruption and to minimize unplanned system down time, it is recommended that your NTM host be rebooted once a month.

Contents

This section contains the following topics:

□

Starting the NTM application

Instructions

Follow these steps to start the NTM application:

1 Log in as `nmadm` to become the network management administrator.

2 Enter `startsys` at the *Linux* operating system shell prompt.

END OF STEPS

□

Stopping the NTM application

Instructions

Follow these steps to stop the NTM application:

1 Log in as `nmadm` to become the network management administrator.

2 Enter `stopsys` at the *Linux* system shell prompt if the system is running.

END OF STEPS

Important! If any pages are running when you execute `stopsys`, you must restart those pages after you execute `startsys`.

□

Starting and stopping the map data server

Overview

Purpose

The Map Data Server (Network Overview Data Server) starts automatically after a reboot.

After that time, if you need to stop or start the server from the command line, you should follow these procedures.

Contents

This section contains the following topics:

□

Starting the map data server

Instructions

Follow these steps to start the map data server:

1 Login as `nmadm`

2 Enter `/nm/web/other-bin/start_n_o_server`

END OF STEPS

□

Stopping the map data server

Instructions

Follow these steps to start the map data server:

1 Login as `nmadm`

2 Enter `/nm/web/other-bin/stop_n_o_server`

END OF STEPS

□

Halting and booting the system

Overview

Purpose

Typically, there are two different procedures for halting the system, one to enter an automatic reboot sequence once the system is halted, and one that shuts down the system. There is also a procedure to manually boot the system.

During emergency conditions, the system must be booted from single user mode.

Recommended rebooting schedule

Alcatel-Lucent recommends that the NTM system be rebooted on a regularly scheduled basis (once a month is highly suggested).

The reasoning behind this recommendation is as follows:

- execution of machine dependent diagnostics to verify hardware integrity
- execution of operating system filesystem checks
- execution of OS and application initialization
- verify/maintain familiarity with local system procedures
- reset and verify interfaces to networks and other applications including non-Alcatel-Lucent software
- minimize unplanned system downtime.

Contents

This section contains the following topics:

□

Normal halting and booting procedures

Overview

Purpose

The following Halting and Booting procedures are those typically used when administering NTM.

Contents

This section contains the following topics:

□

Halting the system processes with automatic reboot

Instructions

Follow these steps if you want your system to reboot automatically.

1 Log in as `nmadm`

Hint: It is always a good idea to send a wall message notifying users of the reboot.

2 Enter `stopsys` to stop the NTM application.

3 From the system console, log in as `root`.

Hint: Although this can be done from a remote location, it is better to do this at the system console so system messages can be viewed.

4 Enter `shutdown -r grace_period`

Hint: `grace_period` is the number of minutes allowed for users to log off the system.

Result: After the grace period ends, the system shutdown starts.

5 Do not interrupt the autoload sequence.

Result: The system will automatically restore to multiuser mode in 20 to 30 minutes.

6 Log in as `nmadm` (or equivalent) and enter `startsys` to restart the NTM application.

END OF STEPS

□

Halting the system processes without automatic reboot

Instructions

Follow these steps if you DO NOT want your system to reboot automatically; otherwise, see "Booting a halted system manually" (p. 16)

1 Log in as `nmadm`

Hint: It is always a good idea to send a wall message notifying users of the reboot.

2 Enter `stopsys` to stop the NTM application.

3 Log in as `root` at the system console.

Hint: Although this can be done from a remote location it is better to do this at the system console so system messages can be viewed.

4 Enter `shutdown -h grace_period`

Hint: `grace_period` *is the number of minutes allowed for users to log off the system.*

Result: After the grace period ends, the system shutdown starts. Once the system halts, a message will be displayed on the console.

5 The system may now be powered down. Switch off the system using the power button located at the top the cabinet.

END OF STEPS

□

Booting a halted system manually

Instructions

Follow these steps to boot a halted system manually:

1 Switch on the system using the power button located at the top the cabinet.

Hint: The system takes 20 to 30 minutes to come up.

Result: After the system comes up, you receive the `login` prompt on the console.

END OF STEPS

□

5 Backing Up and Restoring the System

Overview

Purpose

This chapter provides information and procedures required for:

- backing up the system,
- archiving data to a central archive area,
- administering the archive area.
- restoration on both the NTM and Report Writer hosts.

Contents

This chapter contains the following topics:

Backup and Restore Overview

Introduction

While the Linux port of NTM is able to support more hardware configurations, this flexibility results in more variation in how certain tasks are accomplished. The mechanisms used to backup and restore data depend upon a number of factors, including whether or not the machine is virtualized, whether the disks are local or remote (e.g. SAN), whether logical volumes or partitions are utilized, as well as the type of backup hardware that will be utilized. In some cases, an NTM-recommended procedure can be utilized, while in others local procedures must be used either due to IT mandates or access restrictions.

Scope

The backup and restoral procedures are divided the same way as they are for the HP-UX port, with separate procedures for the root file system, application and system data, and databases. Since the make_tape_recovery and fbackup utilities are specific to HP-UX, only the database backup and restoral procedures (using arcmanager) are the same for Linux and HP-UX (arcmanager on Linux additionally supports backups to disk). There are multiple procedures for handling root file system backups, depending on the system configuration. The application and system data backups are independent of system configuration.

All procedures use standard tools which are documented in the OS Administration Guide, manual pages, and other documentation. The procedures described here should be considered the starting point for the local mechanism, rather than authoritative. The only exceptions are the procedures for “arcmanager”. For an overview of the standard administration procedures, the Red Hat Enterprise Linux System Administration Guide (http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/en-US/System_Administration_Guide_/) should be consulted.

Alternative Mechanisms

In addition to tools described here, 3rd-party tools should also be considered as a part of the complete backup and recovery solution. A few recommended tools include:

- Amanda - http://www.amanda.org/ - This package is included in RHEL5, but is not installed by default. It can be used to backup multiple machines, and supports a large variety of devices for backup medium. It uses standard formats, such as dump and tar, for its backups they can be read even on systems that do not have Amanda installed.

Commercial support is available, as are modules for specific types of backups, such as Oracle database data. It requires some initial configuration, but is easy to use once it is set up.

- Bacula - http://www.bacula.org/en/ - This is another free package, but it is not included with RHEL5. It provides an easy to use GUI, and is fairly simple to configure. It uses a proprietary storage format, so the backups are only able to be read by Bacula. It is a bit less flexible than Amanda, but is still a powerful, stable, and useful tool to consider.
- G4L (Ghost for Linux) - http://sourceforge.net/projects/g4l/ - This package is actually a bootable disk which can be used to create or restore an image of a disk to and from another local disk or an FTP location. It can automatically compress data during transfer. It has limited use, but can be very useful for handling the backup of the disk containing the root file system.

Hardware

As with the HP-UX port, NTM recommends the inclusion of a tape drive, but does not require it. Multiple tape solutions are available, as well as removable disks, NFS or FTP accessed remote storage, SAN backups, and network backup applications (such as Amanda). Some tape drives are supported with the default RHEL installation, while others may require the addition of a driver supplied by the vendor. The procedures described here largely refer to the use of a tape drive. It is expected that an appropriately sized unit is chosen, and that it has adequate throughput to meet the performance needs. Table 1 provides some specs on some popular tape technologies. Note that all modern tape drives are capable of compression, so advertised numbers may be significantly higher (typically twice as large) than the values in the Transfer Rate and Native Media Capacity columns.

Table 1 Media Type specification

Media Type	Drive Type	Native Media Capacity (GB)	Transfer Rate (GB/hr)
DDS-1	DAT	2	2
DDS-2	DAT	4	2.8
DDS-3	DAT	12	5.4
Travan 40	Travan	20	14.4
DDS-4	DAT	20	11
VXA-1	Exabyte	33	11
DAT-72	DAT	36	13
DLT IV	DLT8000	40	22
VXA-2	Exabyte	80	22
Half-high Ultrium 1	LTO 1	100	27
Ultrium 1	LTO 1	100	54
Super DLT 1	SDLT 220	110	40
VXA-3	Exabyte	160	43
Super DLT I	SDLT 320	160	58
Ultrium 2	LTO 2	200	108
Super DLT II	SDLT 600	300	127
VXA-4	Exabyte	320	86
Ultrium 3	LTO 3	400	216
Ultrium 4	LTO 4	800	288
Ultrium 5 (2010)	LTO 5	1600	324

□

Recommended backup schedule

Table

Table 2 shows the recommended backup and archiving schedule for NTM (assuming eight days of historical data).

> **Reference:** For Report Writer backup schedule, see the “Backing Up the Database” section in the *Report Writer Guide*.

Table 2 Recommended backup schedule

Operation	System State	Schedule	Approximate Time to Complete
Full/incremental backup of all file systems	Multiuser mode (The *Linux* system is running, applications may be running, all valid users can log in.)	`AUTOMATICALLY:` `MANUALLY:` After the NTM is loaded, or the system is configured and fully operational, after any software updates are installed by customer support, or after any major change to the software.	Three Hours
Backup of Root Disk	Multiuser mode (The *Linux* system is running. The NTM system is stopped. Users are suggested to refrain from using the host or limiting user activity.)	After new *Linux* is loaded (i.e. a complete *Linux* load of patches to the current *Linux* release). It recommended that this backup be done ***every 3 months*** to provide a current copy of the root disk backup. This is the preferred method as it only requires stopping the NTM application (`stopsys`) before making this backup.	One Hour
Archive of historical data	Collecting data (The *Linux* system is running, applications are running, all valid users can log in.)	Depends on the operation of the center. This data is not required unless you want to analyze or generate reports on data that is more than eight days old. **Reference: Reference:** “Saving historical data to the archive” (p. 10)	Varies by size of data being backed up.

□

Backup and Archive methods

Overview

Definition

NTM considers a ***backup*** as a process of copying the contents of specified file systems onto magnetic tapes. Backing up information onto tape protects data in case of a system failure. NTM also has a process referred to as ***archiving*** data. This is the process of storing historical data in a designated area on the NTM host. Data in the archive area can be accessed from the NTM GUI.

Methods

There are a few scenarios for backup and recovery of the NTM system:

- If the root file system is a virtual disk, and NTM is installed as a Virtual Machine (VM), then the host machine/environment must be used to backup and recover the root file system.
- If the root file system is on a remote disk, such as a SAN, then the backup and recovery mechanism should be done on the machine or device that hosts the actual disk space.
- If the root file system is on a local disk, then the following procedures can be used. The appropriate procedure depends upon the type of space used for the file system. If the root file system is in a normal disk partition, then the partition backup and recovery procedure may be used. If the root file system is in a logical volume, then the full disk backup and recovery procedure is required.
- Archive historical data using the NTM `arcmanager` utility. The custom utility can be used to:
  - save a portion, or all of a historical database to either the archive area, tape or disk files.
  - save an archive database to tape or disk files.

Important! If you have questions, contact customer support to help you choose the most appropriate file restoration strategy.

Related Functions of the arcmanager utility

In addition to the backup and archive functions of the NTM arcmanager utility, the `arcmanager` utility can also:

- restore data from tape.

- restore data from disk files.
- purge databases from the archive area.
- See “Purging archive data” (p. 64).
- list the NM databases
  See “Listing the databases” (p. 66).

Contents

This section contains the following topics:

□

The NTM data archive

Storing Historical database information in the archive

The NTM custom `arcmanager` utility allows users to store all, or part of the historical databases in an archive area. Having an archive on the host allows the flexibility to store network event data which can be used for training, system performance monitoring, or future reference. By having the data stored on the system, it can be retrieved more quickly. Data stored in archive area isn't automatically purged.

Other Archive functions

Administration of the system archive area is also performed using the `arcmanager` utility. Archive functions that can be performed with the arcmanager utility:

- "Purging archive data" (p. 64)
- saving the data in the archive to tape
- saving the data in the archive to disk files
- restoring data on tape to the archive area
- restoring data from disk files to the archive area

Purging archive data

Each data entry in the archive can be purged using the "Purging archive data" (p. 64).

Saving Archive Data to Tape or Disk File

Since the data stored in the archive was defined when it was placed in the archive, a complete archive entry must be saved when storing the information to tape or disk files.

Restoring Archive Data from Tape or Disk File

When restoring data from tape or disk files to the NTM system, the data must be placed in the archive area.

> **Important!** You cannot restore historical data to the historical databases unless the databases on the NTM host have been compromised and removed in a system failure. Only in this case can information be restored in it's entirety to the historical database area of the system.

Saving historical data to the archive

Purpose

Using the NTM `arcmanager` utility users can store all or part of any of the historical databases in an archive area so that it can be retrieved and viewed via the GUI.

Instructions

Follow these steps to store historical data in the archive:

1 Access the `arcmanager` menu using one of the methods in "Accessing arcmanager" (p. 57)

Result: The screen will show the following menu:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  6) Exit the backup program
```

2 Enter "1" at the "Enter Choice" prompt.

Result: The system displays the data available on the system which can be archived.

```
Select database to be saved to archive area, tape or on disk

1) start:  04/20/2005-10:50  end:  04/20/2005-23:55
2) start:  04/21/2005-00:00  end:  04/21/2005-23:55
3) start:  04/22/2005-00:00  end:  04/22/2005-23:55
4) start:  04/23/2005-00:00  end:  04/23/2005-23:55
5) start:  04/24/2005-00:00  end:  04/24/2005-23:55
6) start:  04/25/2005-00:00  end:  04/25/2005-23:55
7) start:  04/26/2005-00:00  end:  04/26/2005-23:55

Enter -  database number  to select an entire database or
      -  r  to specify a different time range for backup
      -  q  to return to main menu

Enter number,  "r", or  "q":
```

3 Follow the decision tree:

- Enter “q” to quit the archive process.

  Stop - End of this procedure.
- Enter the historical database number to be archived, continue with Step 6 .

  Note: The number of databases available depends on your local practices.
- Enter “r” to select specific period for the archive, continue with Step 4

4 Enter the start time for the archive.

5 Enter the end time for the archive.

> **Important!** The archive cannot exceed 24 hours in duration however it can span more than one historical database.
>
> For archive purposes, each day ends at 12:00 midnight. If the archive you request spans two days, the archive will be split into two archives, one for each day.

6 You have the option to change the default archive name. Rename the archive or enter `Return` to accept the default archive name.

Hint: The default name for the archive will reflect the start and end time for the database selected.

7 At the “`Create archive in archive area, tape, disk or quit? [a,t,d,q]:`” Select “`a`” to store the data in the archive

```
The system responds with:
   Output will be written to the Archive Log. Should it be displayed here
   also? [y,n] (Default is y):
```

Enter “n” to directly proceed with the archive process.
Enter “y” to display the information to the screen as the archive is in progress.

> **Result:** The estimated size of the archive is displayed.

8 After the size of the archive is displayed, you will be prompted with:

```
Do you wish to proceed? [y/n]
```

Enter “n” to stop the archive process and return to the main menu.

Enter “y” to store the data requested to the archive area.

END OF STEPS

□

Backing up historical data to tape

Purpose

Using the NTM `arcmanager` utility users can store all or part of any of the historical databases to tape.

Important! It is recommended to use DDS-3 tapes for all system and historical backups.

Instructions

Follow these steps to store historical data to tape:

1 Access the `arcmanager` menu using one of the methods in "Accessing arcmanager" (p. 57)

Result: The screen will show the following menu:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  6) Exit the backup program
```

2 At the "Enter Choice" prompt, select "1"

Result: The system responds with a list of historical databases, for example:

```
Select database to be saved to archive area, tape or on disk

1) start:  04/20/2005-10:50  end:  04/20/2005-23:55
2) start:  04/21/2005-00:00  end:  04/21/2005-23:55
3) start:  04/22/2005-00:00  end:  04/22/2005-23:55
4) start:  04/23/2005-00:00  end:  04/23/2005-23:55
5) start:  04/24/2005-00:00  end:  04/24/2005-23:55
6) start:  04/25/2005-00:00  end:  04/25/2005-23:55
7) start:  04/26/2005-00:00  end:  04/26/2005-23:55

Enter -  database number  to select an entire database or
      -  r  to specify a different time range for backup
      -  q  to return to main menu
```

```
Enter number,  "r", or  "q":
```

3 Follow the decision tree:

- Enter “q” to quit the archive process.

  Stop - End of this procedure.

- Enter the historical database number to be stored to disk, continue with Step 6 .

  Note: The number of databases available depends on your local practices.

- Enter “r” to select specific period for the archive, continue with Step 4

4 Enter the start time for the archive.

5 Enter the end time for the archive.

Important! The archive cannot exceed 24 hours in duration however it can span more than one historical database. If you select a period that spans 12:00 a.m., then the program will store the date in two sections, one for each day included in the archive.

6 You have the option to change the default archive name. Rename the archive or enter `Return` to accept the default archive name.

Hint: The default name for the archive will reflect the start and end times for the database selected.

7 At the “`Create archive in archive, tape, disk or quit? [a,t,d,q]:`” Select “`t`” to store the historical data directly to tape.

Result: The system displays the tape drives available on your system.

8 Enter the tape drive name or number from the list displayed.

9 You will be prompted to place a tape in the tape drive you selected:
Load the tape onto tape drive <*drive_name*>. Press <RETURN> when ready. Select `Return.`

```
The system responds with:
   Output will be written to the Archive Log. Should it be displayed here
   also? [y,n] (Default is y):
   Enter "n" to proceed with backup to tape.
   Enter "y" to display the information to the screen.
```

Result: The estimated size of the archive is displayed.

10 Remove the tape when the backup has completed.

11 Label the tape with the contents and date.

END OF STEPS

□

Backing up archive data to tape

Purpose

Using the NTM `arcmanager` utility users can store archived data to tape.

Important! It is recommended to use DDS-3 tapes for all archive data backups.

Instructions

Follow these steps to store archive data to tape:

1 Access the `arcmanager` menu using one of the methods in "Accessing arcmanager" (p. 57)

Result: The screen will show the following menu:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  6) Exit the backup program
```

2 At the "Enter Choice" prompt, select "2"

Result: The system responds with a list of current archives, for example:

```
Select archive to be saved to tape or disk

1)  Archive_1:  start:  03/17/2005-19:00  end:  03/17/2005-20:00
2)  NM20050321_0800__20050321_0805:  start: 03/21/2005-08:00 end:
   03/21/2005-08:05
3)  NM20050321_1910__20050321_1925:  start: 03/21/2005-19:10 end:
   03/21/2005-19:25
4)  MACTEST4:  start:  03/25/2005-07:00  end:  03/25/2005-07:00
5)  MACTEST5:  start:  03/26/2005-07:00  end:  03/26/2005-07:00

Enter archive number, or "q" to return to main menu:
```

3 Follow the decision tree:

- Enter “q” to quit the archive process.

  Stop - End of this procedure.

- Enter the archive number to be written to tape.

4 At the “`Save archive area to tape, disk or return to main menu? [t,d,q]:`” Select "t" to store the archive data directly to tape.

5 Enter the tape drive name or number from the list displayed.

6 You will be prompted to place a tape in the tape drive you selected:
Load the tape onto tape drive <*drive_name*>. Press <RETURN> when ready. Select `Return.`

```
The system responds with:
   Output will be written to the Archive Log. Should it be displayed here
   also? [y,n] (Default is y):
   Enter “n” to proceed with backup to tape.
   Enter “y” to display the information to the screen.
```

Result: The size of the archive is displayed.

7 Remove the tape when the backup has completed.

8 Label the tape with the contents and date.

END OF STEPS

□

Backing up historical data to disk

Purpose

Using the NTM `arcmanager` utility users can store all or part of any of the historical databases to disk files.

Important! It is recommended to use separate partition or disk for disk backups.

Instructions

Follow these steps to store historical data to disk:

1 Access the `arcmanager` menu using one of the methods in "Accessing arcmanager" (p. 57)

Result: The screen will show the following menu:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  6) Exit the backup program
```

2 At the "Enter Choice" prompt, select "1"

Result: The system responds with a list of historical databases, for example:

```
Select database to be saved to archive area, tape or on disk

1) start:  04/20/2005-10:50  end:  04/20/2005-23:55
2) start:  04/21/2005-00:00  end:  04/21/2005-23:55
3) start:  04/22/2005-00:00  end:  04/22/2005-23:55
4) start:  04/23/2005-00:00  end:  04/23/2005-23:55
5) start:  04/24/2005-00:00  end:  04/24/2005-23:55
6) start:  04/25/2005-00:00  end:  04/25/2005-23:55
7) start:  04/26/2005-00:00  end:  04/26/2005-23:55

Enter -  database number  to select an entire database or
      -  r  to specify a different time range for backup
      -  q  to return to main menu
```

```
Enter number,  "r", or  "q":
```

3 Follow the decision tree:

- Enter “q” to quit the archive process.

  Stop - End of this procedure.
- Enter the historical database number to be stored to disk, continue with Step 6 .

  Note: The number of databases available depends on your local practices.
- Enter “r” to select specific period for the archive, continue with Step 4

4 Enter the start time for the archive.

5 Enter the end time for the archive.

> **Important!** The archive cannot exceed 24 hours in duration however it can span more than one historical database. If you select a period that spans 12:00 a.m., then the program will store the date in two sections, one for each day included in the archive.

6 You have the option to change the default archive name. Rename the archive or enter `Return` to accept the default archive name.

Hint: The default name for the archive will reflect the start and end times for the database selected.

7 At the “`Create archive in archive, tape, disk or quit? [a,t,d,q]:`” Select “`d`” to store the historical data directly to disk.

8 The system responds with:

```
Output will be written to the Archive Log. Should it be displayed here
also? [y,n] (Default is y):
```

Enter “n” to proceed with backup to disk.
Enter “y” to display the information to the screen.

> **Result:** The estimated size of the archive and free disk space in HISTBACKUP directory is displayed.

9 Disk backup will be placed in directory (under HISTBACKUP directory) named same as the archive name specified.

Hint: The HISTBACKUP directory (if changed from default) needs to be accessible and writable by nmadm user.

END OF STEPS

□

Backing up archive data to disk

Purpose

Using the NTM `arcmanager` utility users can store archived data to disk files.

Important! It is recommended to use separate partition or disk for disk backups.

Instructions

Follow these steps to store archive data to disk:

1 Access the `arcmanager` menu using one of the methods in "Accessing arcmanager" (p. 57)

Result: The screen will show the following menu:

```
BACKUP AND RESTORE ROUTINES

   1) Save historical data
   2) Save archive data
   3) Restore data
   4) Purge archive data
   5) List the NM databases
   6) Exit the backup program
```

2 At the "Enter Choice" prompt, select "2"

Result: The system responds with a list of current archives, for example:

```
Select archive to be saved to tape or disk

1)  Archive_1:  start:  03/17/2005-19:00  end:  03/17/2005-20:00
2)  NM20050321_0800__20050321_0805:  start: 03/21/2005-08:00 end:
   03/21/2005-08:05
3)  NM20050321_1910__20050321_1925:  start: 03/21/2005-19:10 end:
   03/21/2005-19:25
4)  MACTEST4:  start:  03/25/2005-07:00  end:  03/25/2005-07:00
5)  MACTEST5:  start:  03/26/2005-07:00  end:  03/26/2005-07:00

Enter archive number, or "q" to return to main menu:
```

3 Follow the decision tree:

- Enter “q” to quit the archive process.

  Stop - End of this procedure.
- Enter the archive number to be written to disk.

4 At the “`Save archive area to tape, disk or return to main menu? [t,d,q]:`” Select "d" to store the archive data directly to disk.

5 The system responds with:

```
Output will be written to the Archive Log. Should it be displayed here
also? [y,n] (Default is y):
```

Enter “n” to proceed with backup to disk.
Enter “y” to display the information to the screen.

6 Disk backup will be placed in directory (under HISTBACKUP directory) named same as the archive name specified.

Hint: The HISTBACKUP directory (if changed from default) needs to be accessible and writable by nmadm user.

End Of Steps

□

Root File System Backup

Overview

Purpose

A backup of the root file system is recommended, but not required. If a full file system backup is not made, then a file-level (System and Application Data) backup should be done after the system and application installation is complete.

Some vendors recommend the use of their own procedures to recover a corrupt root file system or to restore data after a disk drive failure. Often, the vendor procedure is easier to use than the generic backup and recovery procedure, and may include vendor-specific drivers and/or partitioning. Thus, the vendor-specific mechanism should be strongly considered. If you wish to use the generic procedure for backup and recovery of the root file system, then continue using this section.

Scenarios

There are a few scenarios for backup and recovery of the root file system.

- If the root file system is a virtual disk, and NTM is installed as a Virtual Machine (VM), then the host machine/environment must be used to backup and recover the root file system.
- If the root file system is on a remote disk, such as a SAN, then the backup and recovery mechanism should be done on the machine or device that hosts the actual disk space.
- If the root file system is on a local disk, then the following procedures can be used. The appropriate procedure depends upon the type of space used for the file system. If the root file system is in a normal disk partition, then the partition backup and recovery procedure may be used. If the root file system is in a logical volume, then the full disk backup and recovery procedure is required.

  Important! This backup is set up when the system is installed. It is scheduled to take place at a time chosen by the customer. It is the customer's responsibility to load backup tapes daily and ensure that these tapes are correctly labeled.

Contents

This section contains the following topics:

Full Root Disk Backup

Purpose

This procedure requires that the system be shut down and booted off of a DVD. The system will be unavailable throughout the backup procedure. The length of time required for this operation is dependent on both the disk speed and backup mechanism throughput.

Instructions

Follow these steps to execute full root disk backup:

1 Insert the Red Hat Enterprise Linux CD into the DVD drive and reboot the system. If the machine is not configured to automatically boot off of the optical drive, then select the drive from the machines Boot Menu.

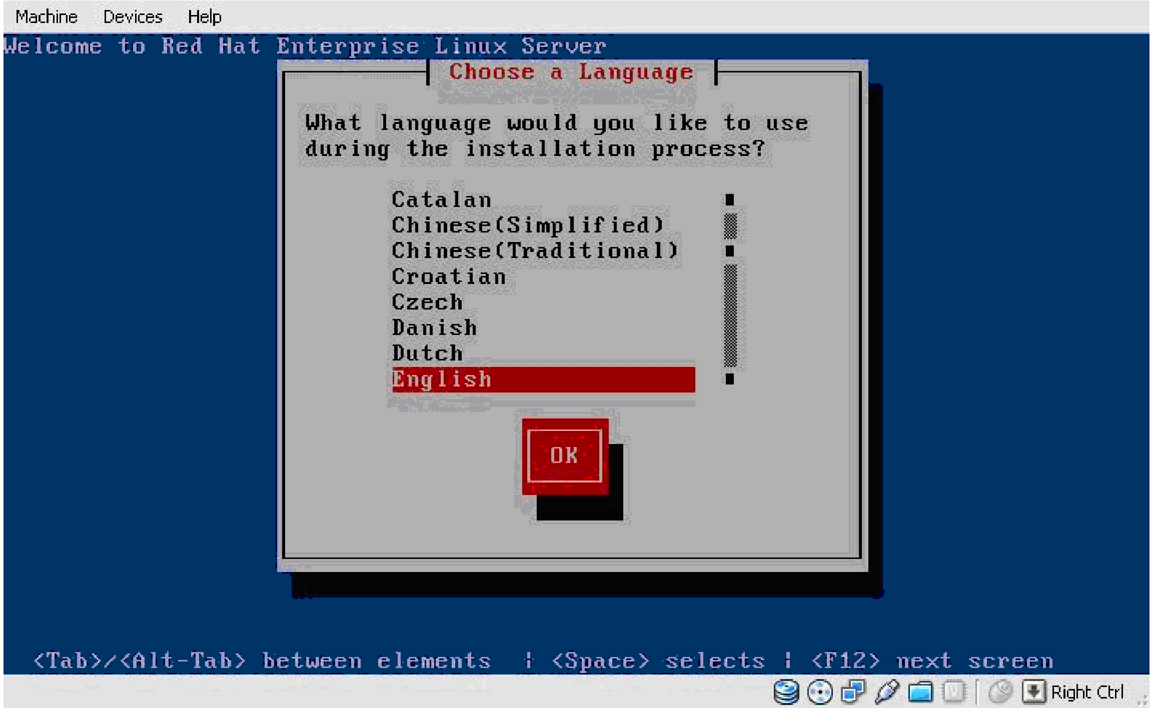
Result: The machine will boot off of the DVD and present a welcome screen with a prompt.

2 Enter `linux rescue`

Result: Linux will be booted into a RAM disk, with a large amount of output messages displayed.

3 On the dialog box ‘Choose a Language’ (Figure 1), select `English` and click `OK`.

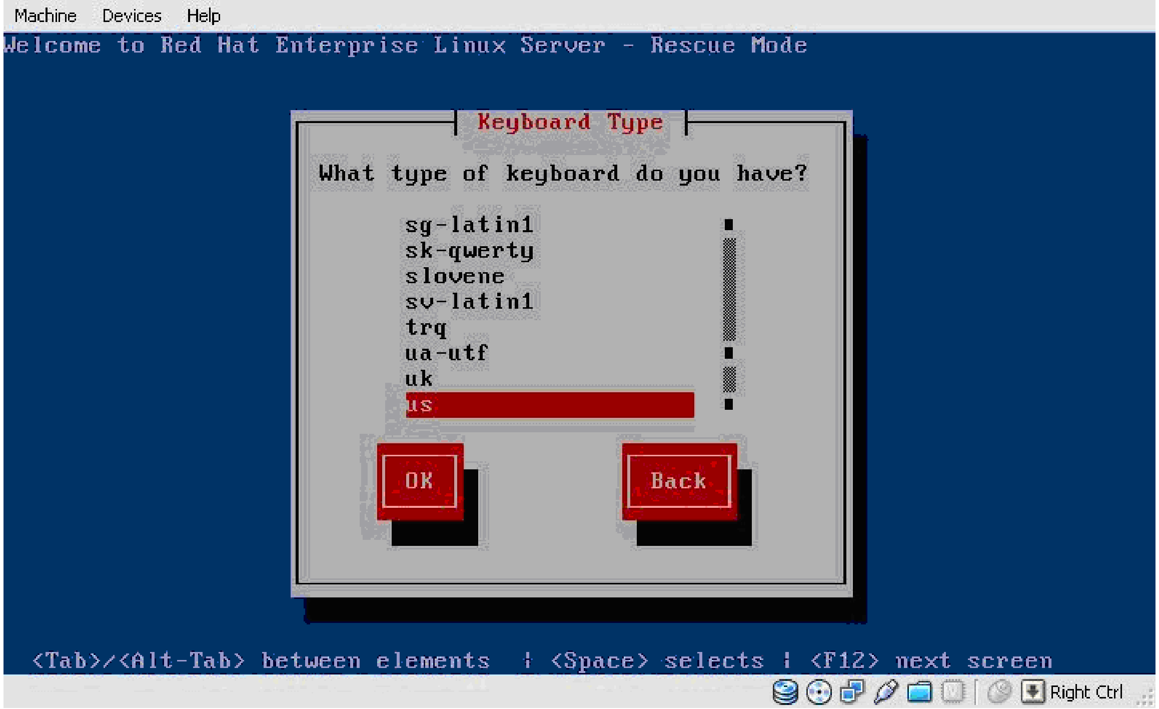
Figure 1 Choose a Language dialog box



```
Welcome to Red Hat Enterprise Linux Server
                 Choose a Language

  What language would you like to use
  during the installation process?

        Catalan
        Chinese(Simplified)
        Chinese(Traditional)
        Croatian
        Czech
        Danish
        Dutch
        English

                 OK

 <Tab>/<Alt-Tab> between elements  | <Space> selects | <F12> next screen
```

4 On the next screen Choose Keyboard type (Figure 2), Select `us` and click `OK`.

Figure 2 Keyboard Type dialog box.



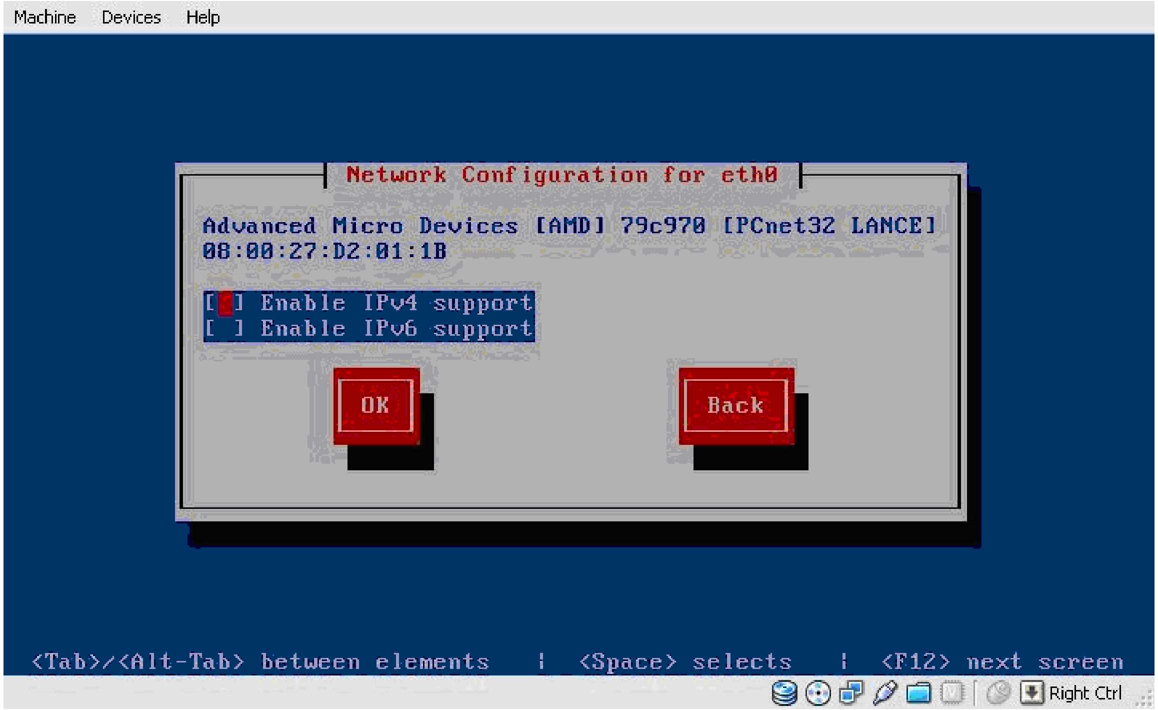
```
Welcome to Red Hat Enterprise Linux Server - Rescue Mode

                    Keyboard Type

        What type of keyboard do you have?

                 sg-latin1
                 sk-qwerty
                 slovene
                 sv-latin1
                 trq
                 ua-utf
                 uk
                 us

               OK                 Back

 <Tab>/<Alt-Tab> between elements  | <Space> selects | <F12> next screen
```

5 On the screen 'Setup Networking' you have an option to start the network interfaces. Answer `Yes` only if you want to store the backup on an NFS connected drive. If you are using a local tape drive, then select `No`.

6 Assuming that you have a network connection on the first interface, select `Yes` on the 'Configure Network Interface' screen.

7 Select `Enable IPv4` support and click `OK` (Figure 3).

Figure 3 Network Configuration dialog box



Network Configuration for eth0

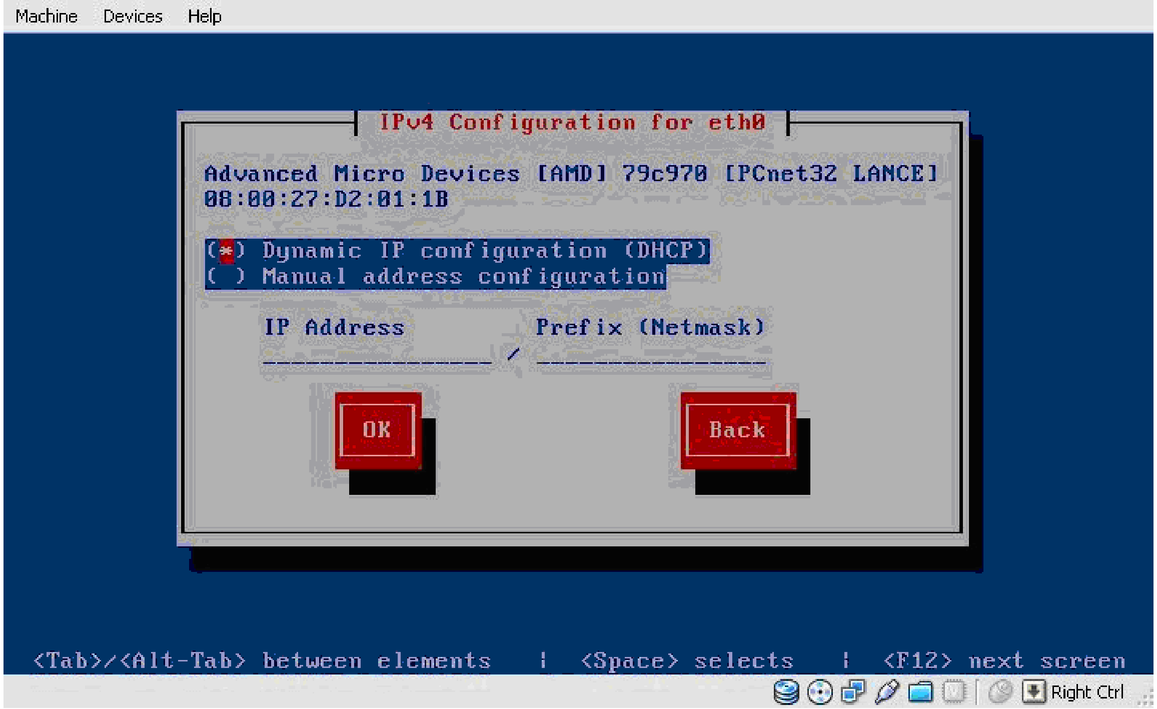
Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
08:00:27:D2:01:1B

[ ] Enable IPv4 support
[ ] Enable IPv6 support

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

8 Figure 4 shows the screen with selection: `Dynamic` or `Manual` configuration, depending upon whether you have a DHCP server available. If you select `Manual` address configuration, then you will need assigned IP address and related information.

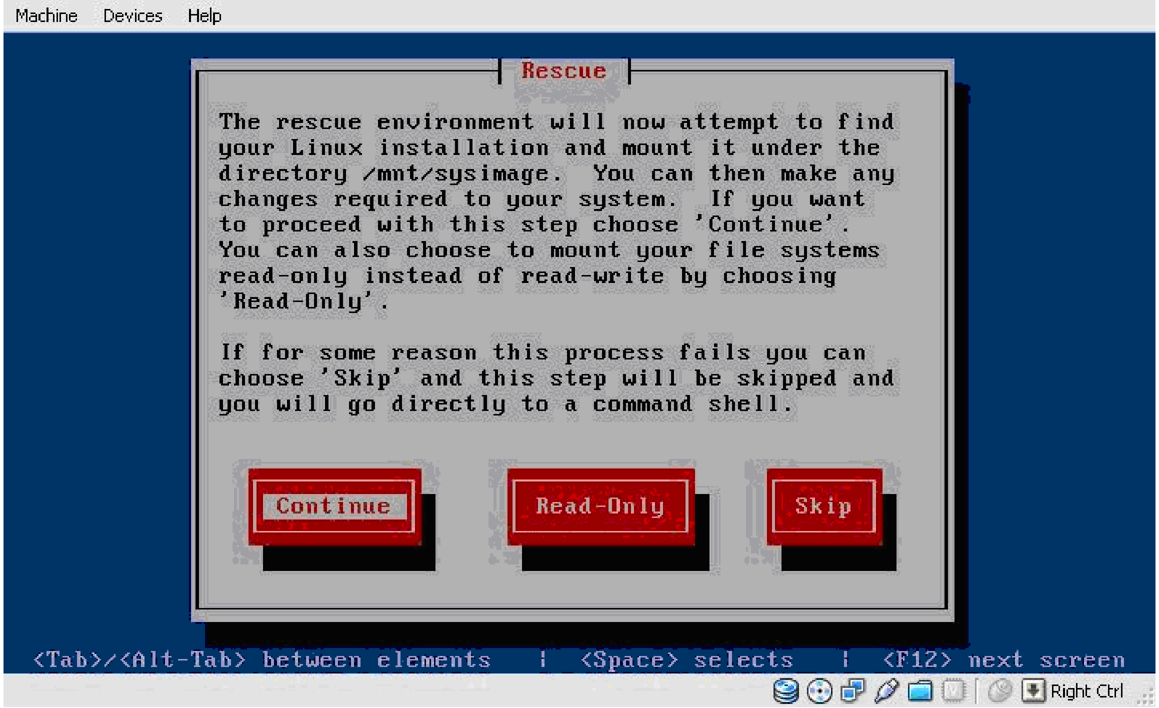
Figure 4 IPv4 Configuration dialog box



```
IPv4 Configuration for eth0

Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
08:00:27:D2:01:1B

(*) Dynamic IP configuration (DHCP)
( ) Manual address configuration

     IP Address              Prefix (Netmask)
     ________________   /   ________________

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

9 Click `Read-Only` when the rescue mode will present the option to search for installations of the OS (Figure 5).

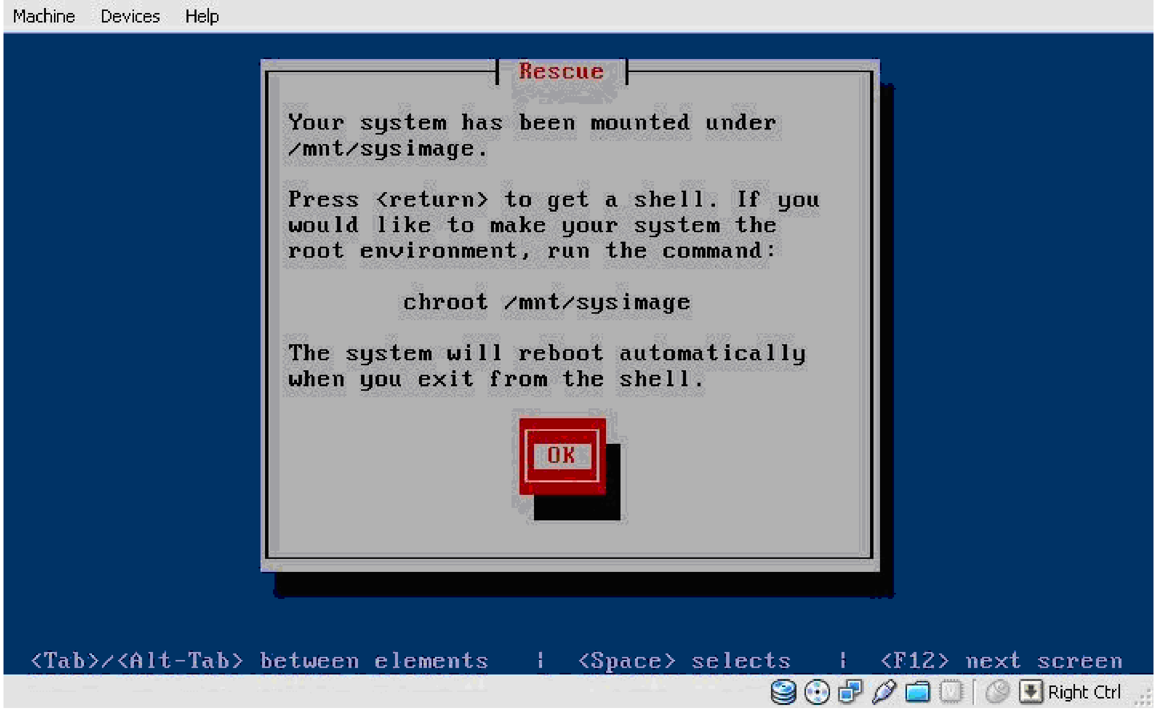
Figure 5 Rescue dialog box



```
Rescue

The rescue environment will now attempt to find
your Linux installation and mount it under the
directory /mnt/sysimage.  You can then make any
changes required to your system.  If you want
to proceed with this step choose 'Continue'.
You can also choose to mount your file systems
read-only instead of read-write by choosing
'Read-Only'.

If for some reason this process fails you can
choose 'Skip' and this step will be skipped and
you will go directly to a command shell.

Continue    Read-Only    Skip

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

10 Upon a successful search for the root disk, it will be mounted on */mnt/sysimage* (Figure 6).

Figure 6 Mounted disk on Rescue dialog box



```
Your system has been mounted under
/mnt/sysimage.

Press <return> to get a shell. If you
would like to make your system the
root environment, run the command:

        chroot /mnt/sysimage

The system will reboot automatically
when you exit from the shell.
```

```
<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

11 Once the final screen is acknowledged, you will be presented with a prompt. The disk file systems will be mounted on */mnt/sysimage*, instead of "/" as they would if you have booted from the disk drives.

Hint: In order to find the root disk on a system that is using logical volumes, you will need to use the `pvdisplay` *command to determine the disk device.*

12 Optional: If you are going to back up the disk using NFS instead of a tape, then you need to mount the file system before executing the backup command.

- Create the mount point using the command: `mkdir /backup`
- Mount the remote file system using the command: `mount <nfsserver>:/<remote name> /backup`, where *`<nfsserver>`* is the name of the remote server, and *`<remote name>`* is the name of the shared directory on the remote NFS server

13 If you are using a tape drive, make sure that you have loaded a tape and know the name of the tape unit's device (e.g. /dev/st0). Copy the data using the dd command

- `dd if=/dev/<root disk> of=/dev/<tape device> bs=1M` (for tape backup) or
- `dd if=/dev/<root disk> of=/backup/rootdisk.img bs=1M` (for NFS backup)

14 When the backup has completed, you may reboot the system to its normal state. From the prompt, type `exit` to begin the reboot.

15 When the system is doing its Power On Self Test (POST), eject the DVD from the optical drive so that it does not attempt to reboot onto the optical media

16 If your machine provides a Boot Menu, then you may use that to force the system to boot onto the boot disk.

END OF STEPS

□

Root File System Backup

Purpose

This procedure is very similar to the Full Root Disk Backup procedure, except for the final steps. You can backup to a local tape or an NFS mounted directory. The advantage of this procedure over the Full Root Disk Backup is that it can take up less space since it only includes the data from the root file system.

Instructions

Follow these steps to execute full root disk backup:

1 Insert the Red Hat Enterprise Linux CD into the DVD drive and reboot the system.
If the machine is not configured to automatically boot off of the optical drive, then select the drive from the machines Boot Menu.

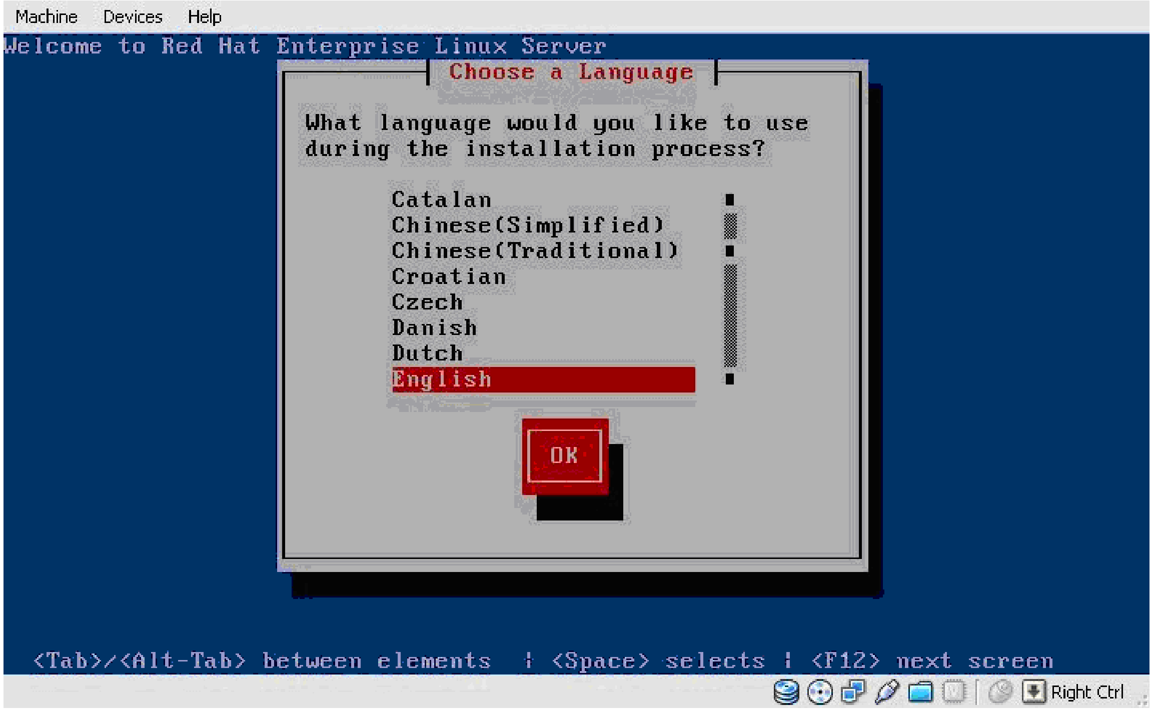
Result: The machine will boot off of the DVD and present a welcome screen with a prompt.

2 Enter `linux rescue`

Result: Linux will be booted into a RAM disk, with a large amount of output messages displayed.

3 On the dialog box ‘Choose a Language’ (Figure 7), select `English` and click `OK`.

Figure 7 Choose a Language dialog box



Welcome to Red Hat Enterprise Linux Server

Choose a Language

What language would you like to use during the installation process?

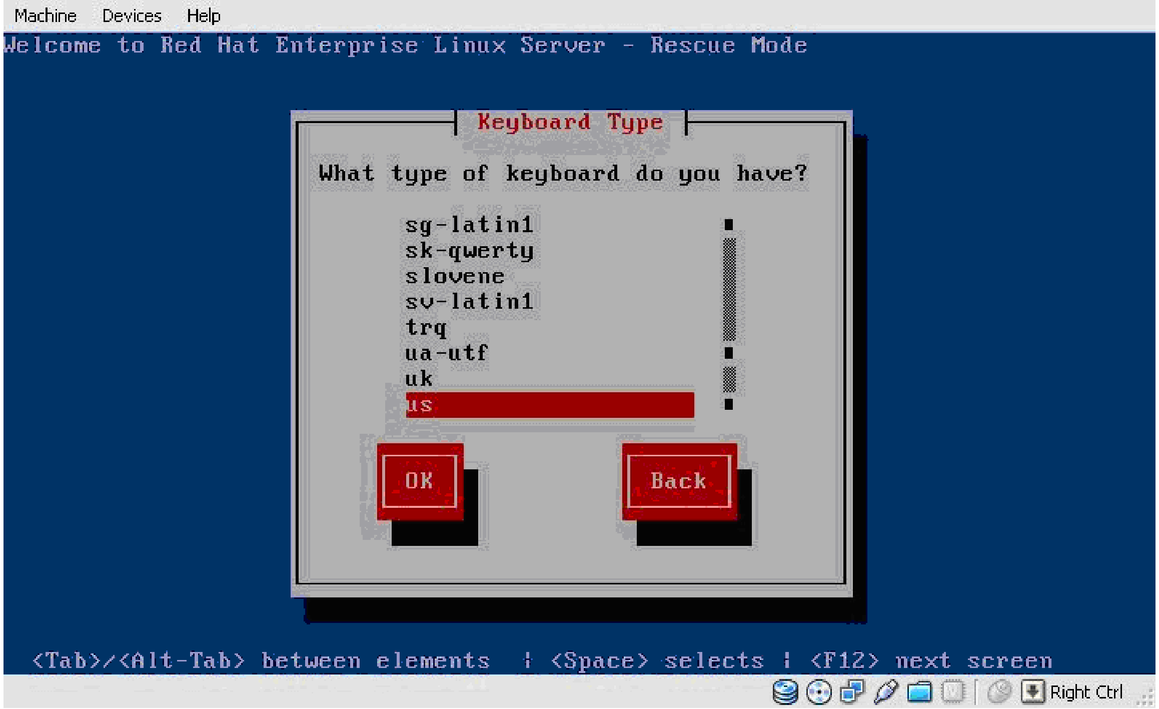
Catalan
Chinese(Simplified)
Chinese(Traditional)
Croatian
Czech
Danish
Dutch
English

OK

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

4 On the next screen Choose Keyboard type (Figure 8), Select `us` and click `OK`.

Figure 8 Keyboard Type dialog box.



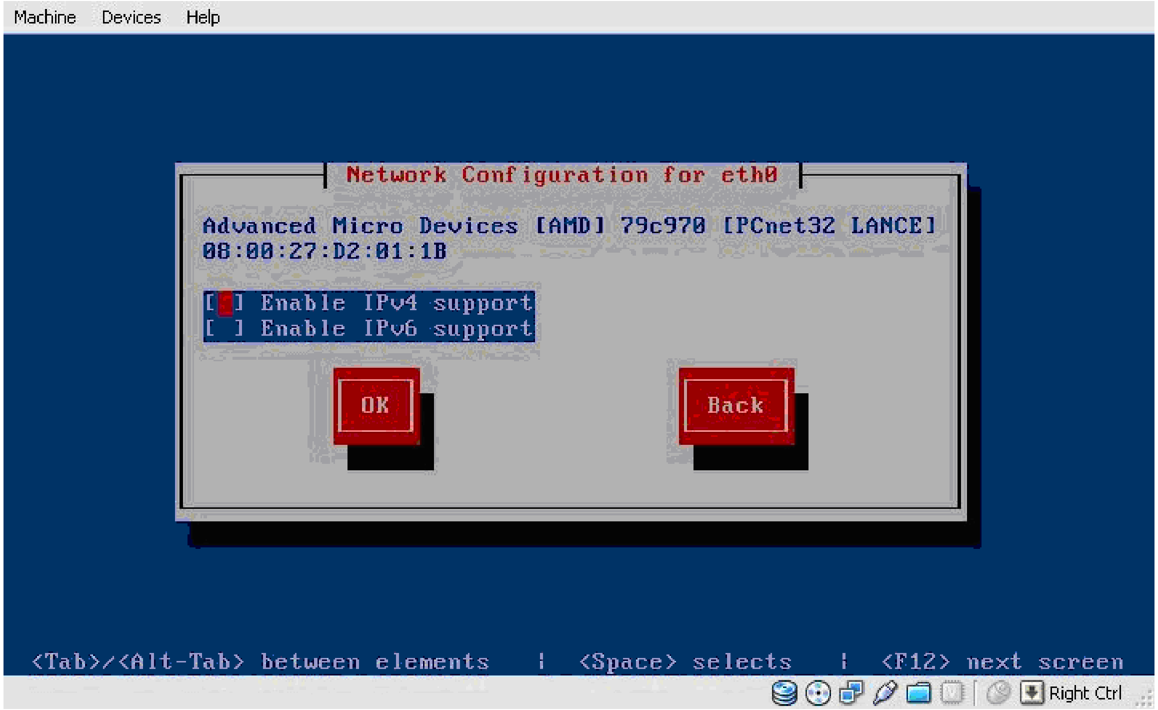
```
Welcome to Red Hat Enterprise Linux Server - Rescue Mode

Keyboard Type

What type of keyboard do you have?

sg-latin1
sk-qwerty
slovene
sv-latin1
trq
ua-utf
uk
us

OK          Back

<Tab>/<Alt-Tab> between elements  | <Space> selects | <F12> next screen
```

5 On the screen ‘Setup Networking’ you have an option to start the network interfaces. Answer `Yes` only if you want to store the backup on an NFS connected drive. If you are using a local tape drive, then select `No`.

6 Assuming that you have a network connection on the first interface, select `Yes` on the ‘Configure Network Interface’ screen.

7 Select `Enable IPv4` support and click `OK` (Figure 9).

Figure 9 Network Configuration dialog box



Network Configuration for eth0

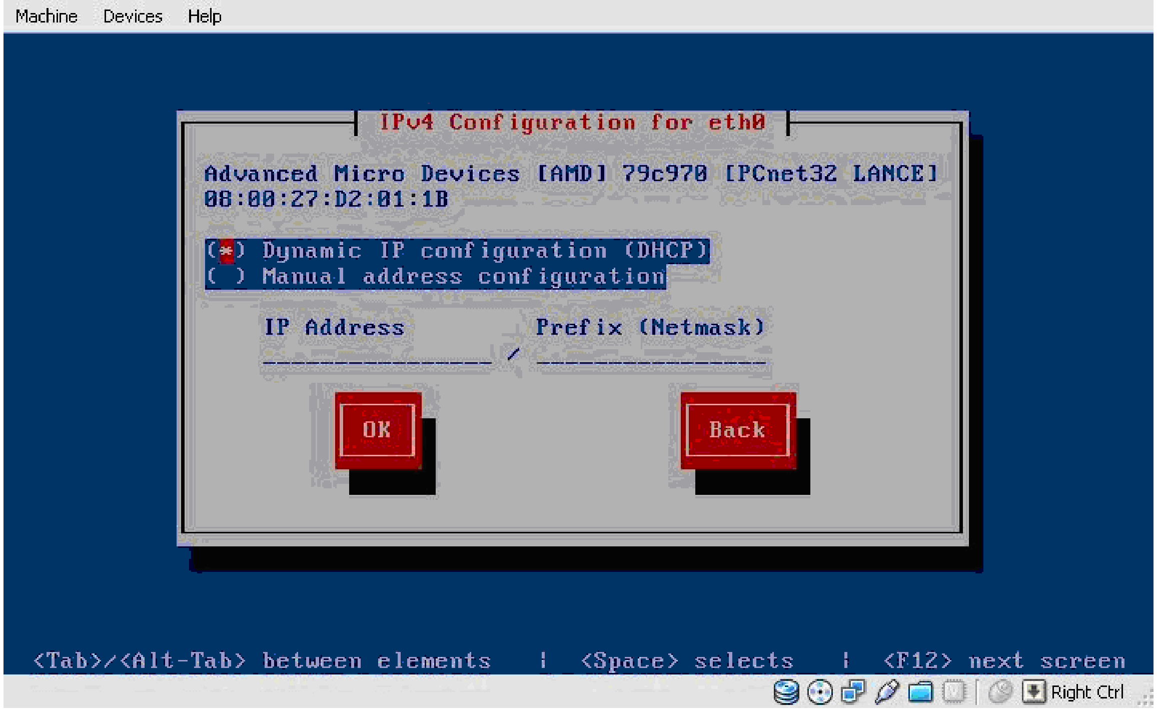
Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
08:00:27:D2:01:1B

[ ] Enable IPv4 support
[ ] Enable IPv6 support

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

8 Figure 10 shows the screen with selection: `Dynamic` or `Manual` configuration, depending upon whether you have a DHCP server available. If you select `Manual` address configuration, then you will need assigned IP address and related information.

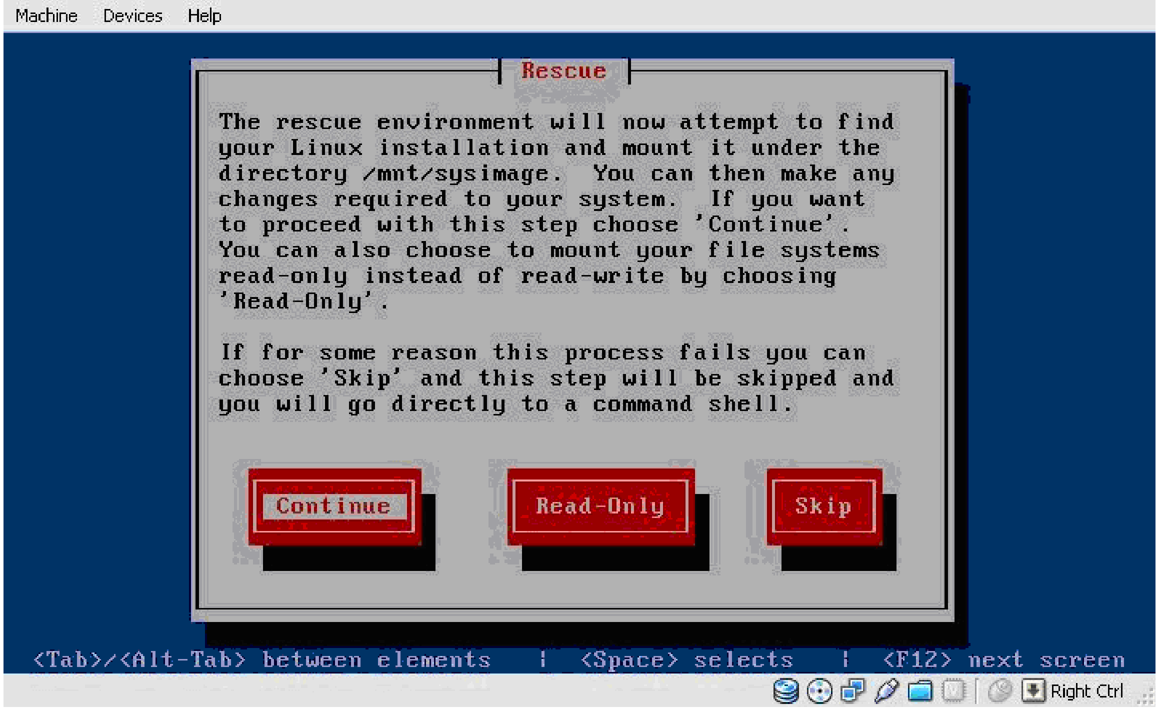
Figure 10 IPv4 Configuration dialog box



```
IPv4 Configuration for eth0

Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
08:00:27:D2:01:1B

(*) Dynamic IP configuration (DHCP)
( ) Manual address configuration

IP Address          Prefix (Netmask)
_________________ / _________________

OK          Back

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

9 Click `Read-Only` when the rescue mode will present the option to search for installations of the OS (Figure 11).

Figure 11 Rescue dialog box

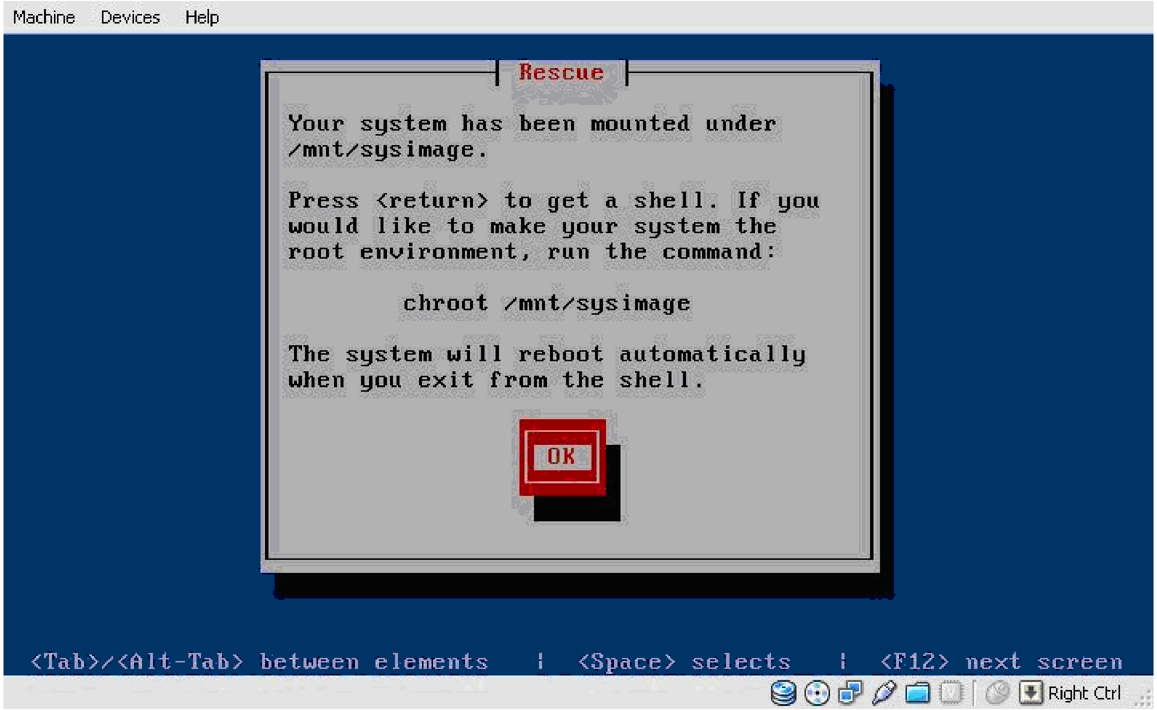


```
The rescue environment will now attempt to find
your Linux installation and mount it under the
directory /mnt/sysimage.  You can then make any
changes required to your system.  If you want
to proceed with this step choose 'Continue'.
You can also choose to mount your file systems
read-only instead of read-write by choosing
'Read-Only'.

If for some reason this process fails you can
choose 'Skip' and this step will be skipped and
you will go directly to a command shell.
```

Continue
Read-Only
Skip
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
Right Ctrl

10 Upon a successful search for the root disk, it will be mounted on */mnt/sysimage* (Figure 12).

Figure 12 Mounted disk on Rescue dialog box



Your system has been mounted under /mnt/sysimage.

Press <return> to get a shell. If you would like to make your system the root environment, run the command:

```
chroot /mnt/sysimage
```

The system will reboot automatically when you exit from the shell.

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

11 Once the final screen is acknowledged, you will be presented with a prompt. The disk file systems will be mounted on */mnt/sysimage*, instead of "/" as they would if you have booted from the disk drives.

Hint: In order to find the root disk on a system that is using logical volumes, you will need to use the `mount` *command and look for the partition that is mounted on /mnt/sysimage.*

12 While this step is normally conducted when doing system and application data backups, it should be considered at this point as well. The relevant metadata is the boot sector and partition tables. The boot sector should be backed up to an NFS location, USB flash drive, or FTP location, while the partition tables should also be copied, but could be simply printed.

Use the following commands to create the metadata:

```
mkdir /metadata
dd if=/dev/<root disk> of=/metadata/bootsect.img bs=512
   count=1  (where <root disk> is the device containing your
   root file system, such as /dev/sda)
fdisk -l > /metadata/partlist.txt


Copy the contents of /metadata to your destination using cp or
   ftp, as appropriate.
```

13 Typically, the dump command is used for complete file system backups, as it is capable of being used to completely reconstruct the file system once the partition table is restored. Alternatively, tar or cpio can be used if you want to manually create the file system after recovering the partition table. These instructions assume that dump is the desired command.

```
dump -0u -f /dev/<tape device> /dev/<root partition>
```

14 For example, `dump -0u -f /dev/st0 /dev/sda2` would write the contents of */dev/sda2* to the tape device */dev/st0*. It is a level 0 dump, so it is a complete backup of the file system.

15 If you want to copy the data to an NFS-accessible location, then write to a file on the NFS mounted location. For example, `dump -0u -f /backup/root.dump /dev/sda2` would copy the contents of the file system contained in */dev/sda2* to the file */backup/root.dump*, assuming that */backup* is a remotely mounted directory.

16 Execute `exit` command to begin the reboot.

17 When the system is doing its Power On Self Test (POST), eject the DVD from the optical drive so that it does not attempt to reboot onto the optical media.

18 If your machine provides a Boot Menu, then you may use that to force the system to boot onto the boot disk.

END OF STEPS

□

Root File System Recovery

Overview

Definition

Restore is the process of loading a backup tape and reading its contents onto the system.

Archive data can be restored to either the archive area or directly to a historical database. Restoring the data directly to a historical database thereby restores the system to the state it was in when the backup tape was made.

A restore is done in the event of: a system failure, system generic update, orreview of a network event. The procedure for restoring files depends on the reason for restoral.

Contents

This section contains the following topics:

□

Full Root Disk Recovery

Instructions

Follow these steps to execute Full Root Disk Recovery:

1 To get to the recovery mode prompt, follow Steps 1 through 7 of the "Full Root Disk Backup" (p. 25) Procedure.

2 If you are using a tape drive, make sure that you have loaded a tape and know the name of the tape unit's device (e.g. /dev/st0).

3 Use the `dd` command to copy the data.

4 For Tape recovery execute `dd if=/dev/<tape device> of=/dev/<root disk> bs=1M`

5 For NFS recovery execute `dd if=/backup/rootdisk.img of=/dev/<root disk> bs=1M`

6 When the recovery has completed, you may reboot the system to its normal state. Execute `exit` command to begin the reboot.

7 When the system is doing its Power On Self Test (POST), eject the DVD from the optical drive so that it does not attempt to reboot onto the optical media.

8 If your machine provides a Boot Menu, then you may use that to force the system to boot onto the boot disk.

END OF STEPS

□

Root File System Recovery

Purpose

This procedure assumes that you have already recovered the root disk's metadata, or have it available for the recovery process. If you use a vendor's recovery disk, it will usually put the system into a state that will allow you to recover the data without requiring you to perform any additional steps to recover metadata.

Instructions

Follow these steps to execute Root File System Recovery:

1 To get to the recovery mode prompt, follow Steps 1 through 7 of the "Root File System Backup" (p. 33) Procedure.

2 Optionally you can recover metadata. To perform this execute Step 3 to Step 6. Otherwise skip them and go to Step 7.

3 If you have saved the boot sector for the root disk and wish to restore it, you should do this before attempting to restore the root partition data. This should not be done unless the disk has been replaced or the partition table has been corrupted. If your disk has been replaced, but you did not save the boot block, you can use the partition information to manual reconstruct the disk through the use of the fdisk command. To recover the boot block execute the following commands:

```
mkdir /metadata
```

> **Reference:** Boot sector (MBR) may contain boot loader software (GRUB, LILO, etc.) which, when MBR is built from scratch, may need to be reinstalled. More information about bootloaders can be found in: "Reinstalling the Bootloader" section at http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/sysadmin-guide/s1-rescuemode-boot.html

4 copy the *bootsect.img* file from your NFS mounted directory, USB flash drive, or ftp location to */metadata* directory.

5 Execute `dd if=/metadata/bootsect.img bs=512 of=/dev/<root disk> count=1` (where *`<root disk>`* is the device containing your root file system, such as */dev/sda*)

6 If you had to recover the boot sector, you should restart the procedure to ensure that the rescue mode correctly discovers and utilizes the restored partition table.

7 Put your tape into the drive (if not using NFS) before executing the following steps.

Hint: The following steps assume that your root file system is /dev/sda2 and that your tape drive is /dev/st0, you will need to adjust them as needed using your actual locations.

8 Execute `mke2fs -j /dev/sda2`

9 Execute `mkdir /mnt/rootfs`

10 Execute `mount /dev/sda2 /mnt/rootfs`

11 Execute `cd /mnt/rootfs`

12 Execute `restore -rf /dev/st0`

13 When the recovery has completed, you may reboot the system to its normal state.

14 Execute `exit` command to begin the reboot.

15 When the system is doing its Power On Self Test (POST), eject the DVD from the optical drive so that it does not attempt to reboot onto the optical media.

16 If your machine provides a Boot Menu, then you may use that to force the system to boot onto the boot disk.

END OF STEPS

□

System and Application Data Backup

Overview

Purpose

As NTM is more tolerant of a variety of configurations, it is more difficult to specify a single solution for some activities, such as backup/recovery. As discussed in the beginning of this section, multiple solutions exist, with the most applicable one being specific to your machine configuration.

Since the NTM application is normally running, it is expected that most backups should be able to be made on a running system. This can cause problems with backup data integrity, so the chosen solution should be based on consideration of data integrity versus convenience.

Examples are provided using both the dump and tar utilities. The tar utility works similarly to the fbackup utility provided in HP-UX, in that you can provide a list of exclusions. There is an excellent guide for the use of tar at this location:

Tar - http://www.gnu.org/software/automake/manual/tar/tar.html

Backup Scope

The system and application data that should be backed up consists of programs and files that are part of the operating system or NTM application. The databases are not normally included in these backups as they use specific tools to extract their backup data. They may be backed up indirectly, however, since the system may be configured to create “regular” files out of the databases for inclusion in the System and Application Data backup. Finally, temporary data, such as that stored in /tmp, is not normally useful for inclusion in the backups.

The following Table 3 shows possible groups of data that should be backed up.

Table 3 Groups of data to be backed up

Backup Group	Directories	Notes
root	/bin /boot /etc /home /lib /lib64 /opt /root /sbin /usr /var	
musr	/musr	

Backup Group	Directories	Notes
nm	/nm	Could be included in the root backup group, if desired

Backup tools

Whether `dump` or `tar` is being used, the list of directories would be the same. The list is supplied to dump or tar as an argument when backing up a particular group of data. Additional groups could be made if the directories in the root group spanned multiple file systems, especially when dump is being used.

Depending on the backup device, multiple (possibly all) of the backup groups could be kept on a single tape. In this case, the no-rewind version of the device should be utilized for all backup executions except for the last one.

Linux has significant support for the dump command, including a means of noting whether or not a file system should be a candidate for backup (using the fifth field in each row of */etc/fstab*). In addition, the `chattr` and `lsattr` commands can be used to maintain the *`no dump`* flag of a directory or file. Using the command `chattr +d /tmp/somefile` would tell `dump` to skip the file */tmp/<file>* everytime a `dump` is performed.

If `dump` cannot be used, or another tool is desired, then you should consider using `tar` or `cpio`. Be aware, however, that if you are not backing up a snapshot of a file system, that there is some risk of reduced backup integrity due to file system activity during the backup.

Contents

This section contains the following topics:

□

Using the Dump Utility

Purpose

If you are using logical volumes for your file systems, then you can take advantage of the “snapshot” mechanism to help guarantee the integrity of your backups. An LVM snapshot is essentially a copy of the state of a file system at the time the snapshot was made. This is very useful for active file systems since you can make a backup of the snapshot rather than getting potentially corrupt backups from the live file system.

Snapshots are not true copies of their associated file systems. Instead, they contain only the blocks from the original file system that have changed since the snapshot was taken. So, the snapshot doesn’t contain any blocks initially, making its creation nearly instantaneous, but will grow as changes are made to its source file system. There is a slight performance penalty for using snapshots since data that is written to the source file system also needs to be written to each associated snapshot. Because of this, snapshots are created just before the backup and removed as soon as the backup is complete.

In order to create a snapshot, you need to have space for it in the volume group that contains the source file system (logical volume). In general, 1 or 2 gigabytes is fine for a snapshot size, unless the backup is going to take an excessively long time or the file system is very active (for writes and modifications). You should use a simple convention for your snapshots, such as appending the string “_ss” to the name of the logical volume.

The following steps should be applied to each file system that you wish to backup. The steps can be easily scripted and put together to be run each day by cron.

Instructions

Follow these steps to perform the backup using `dump` tool:

1 Execute this command to create a snapshot of the file system:

```
lvcreate --size 1G --snapshot  --name musr_ss /dev/vg00/musr
```

Result: This example shows the creation of a snapshot of the */musr* file system, allocating 1GB of space in the volume group `vg00`. The snapshot will be accessible with the name */dev/vg00/musr_ss*. This snapshot could be mounted on a mount point (e.g. */backup/musr*), but dump does not require this.
While the example shows handling just one file system at a time, you could create all of the snapshots that you need, mount each on a mount point (e.g. */backup*), and then perform the `dump` command on the backup directory (selecting appropriate subdirectories).

2 If you wish to use the dump command, execute this command to perform the backup of the snapshot.

```
dump -0u -f /dev/st0 /dev/vg00/musr_ss
```

Result: This example will perform a level 0 dump (full backup) of the file system contained in /dev/vg00/musr_ss and put the data on the tape located at /dev/st0. The no-rewind device may be needed if you are going to put another backup on the same tape immediately following this one.

3 If you wanted to select particular directories in the file system to backup, then you would need to mount the file system before the dump command is issued. Execute:

```
mount /dev/vg00/musr_ss /backup/musr
```

4 Execute `cd /backup/musr`

5 Execute `dump -0u -f /dev/st0 /backup/musr/fred /backup/musr/mary`

6 If an incremental backup was to be done, then the level would be 1, 2, etc., instead of 0. A level 1 backup is all new or changed data since the last level 0 backup. A level 2 backup is all data that has changed since the last backup of a lower level (0 or 1). The backup levels allow flexibility in determining how much data should be backed up at a particular time.

7 Instead of using the dump command, `tar` or `cpio` could be used. It is recommended that you use snapshots with these commands, if possible. For examples of `tar`, look at the section describing backup/recovery of Standard Partitions.

8 If you mounted the snapshot before running the `dump` command, you need to unmount it before it can be deleted. Execute following commands:

```
cd /
umount /dev/vg00/musr_ss
```

9 Run this command to remove the snapshot:

```
lvremove --force /dev/vg00/musr_ss
```

Hint: Use of the force option is not required except in a script. If it is not used, you will be prompted for acknowledgement before the snapshot is deleted.

END OF STEPS

□

Using the TAR Utility

Purpose

When backups are to be made on a standard partition, and the system has to be left in an operational state (not brought to single-user mode, or booted off of a recovery disk), `tar`, `cpio`, or `pax` should be used instead of `dump`. The `pax` command may be unfamiliar to you, but it is included with Linux, can support `tar` and `cpio` formats (as well as others) and has a large number of options to make it a flexible replacement for the `tar` and `cpio` utilities. The example below uses `tar`, but `cpio` or `pax` could be used in its place (using options appropriate to each utility).

The `tar` utility included with Linux supports a few options to allow you to exclude files, directories, or patterns. This makes the execution of the program easier since you can simply backup starting from the system root (/) and tell tar to skip certain directories.

- `--exclude=/lost+found` (would tell tar to skip the directory /lost+found)
- `--exclude=/lost+found --exclude=/dev` (multiple instances of the option can be used on the tar command line)
- `--exclude-from=/etc/myTarExcludes.txt` (reads the list of files to exclude from the file /etc/myTarExcludes.txt, for example)

It is recommended that you create an exclusion file to reduce the size of the tar command line, if you have several files or directories to exclude. These options can be mixed on the command line, such as in this example:

- `--exclude='*.o' --exclude-from=/etc/local/backupExcl.txt` (don't include any file that ends with ".o", or any files listed in */etc/local/backupExcl.txt*)

Before you begin

This preparation step should be performed only one time. The exclusion file can be named anything. You might have different exclusion files for different backup types. It is recommended that you locate your exclusion files in /etc.

- Create a file /etc/backups/ntmExcl.txt (for example) using vi (or another editor)
- Add the following list of files/directories to the list (this is a suggested list, you may want to add or remove items based on your own needs)
  - /dev
  - /lost+found
  - /mnt
  - /musr/auds
  - /musr/meas

- /musr/log
- /musr/lost+found
- /nm/web/tmp
- /proc
- /rawdata
- /rdbdata1
- /rdbdata2
- /sys
- /tmp
- /var/tmp
- /var/spool/cron/tmp

Instructions

Follow these steps to perform the backup using `tar` tool:

1 Put the appropriate tape in the tape drive. The tape should be of a length appropriate for the planned backup. Now you can perform:

- full backup Step 2
- full backup for use with incremental backups Step 3
- incremental backup Step 4

2 A full backup can be performed by executing the tar command with default options.

```
tar cvpf /dev/st0 --exclude-from=/etc/backup/tarExcl.txt /
```

Hint: Also, consult the guide here, for further information: http://www.gnu.org/software/tar/manual/html_chapter/Backups.html#SEC88

3 If you will be using incremental backups, in addition to full backups, you can use the --listed-incremental option to `tar`. This option will create and use a specified file to keep track of what has been backed up. Execute following commands:

```
rm /etc/backup/fullroot.ssf
tar cvpf /dev/st0 --exclude-from=/etc/backup/tarExcl.txt --
   listed-incremental=/etc/backup/fullroot.ssf /
```

Result: This backup will create a new “snapshot” file containing what was backed up along with timestamps. This file can be used by subsequent incremental backups.

Hint: Also, consult the guide here, for further information: http://www.gnu.org/software/tar/manual/html_chapter/Backups.html#SEC89

4 Assuming that you have a snapshot file already created, you can run the `tar` command and only backup files that were changed since the last backup was run (as determined by the snapshot file). Execute:

```
tar cvpf /dev/st0 --exclude-from=/etc/backup/tarExcl.txt --
  listed-incremental=/etc/backup/fullroot.ssf /
```

Result: This backup will use the data in the indicated snapshot file to determine if a file needs to be backed up. Since we didn't delete the file at the beginning of the step, it will contain the information from the last backup that updated the file.

END OF STEPS

□

System and Application Data Recovery

Purpose

The steps for restoring System and Application Data depend upon whether you used the `dump` or `tar` utility. In either case, restoring data onto a live file system can be tricky. You will not be able to overwrite a file that is in use, so you may have to stop your system or bring it to single user, depending upon the recovery needs. In general, you will not be scripting the restoral of files, so you should become familiar with the command line options and interactive modes, where applicable. Consult the OS user guide as well as referenced guide for the `tar` command.

Recovery from a Dump file

The companion tool to dump is restore. It can be used in both interactive and non-interactive modes. Interactive mode can be very useful if you wish to browse the backup and selectively recover files. The non-interactive mode is usually used when all files from the backup are needed, and the system is at single-user mode (or, perhaps, rescue mode).

Interactive Recovery

An example of recovering data interactively is:

```
cd /musr
restore -if /dev/st0
```

(use commands within dump interactive mode to select and extract files, add and extract)

After “add”ing all files that you wish to recover to the list to be extracted, you run the extract command to restore them to the file system. During the extract, you will be prompted to select the volume to start with. You will normally answer with volume “1” to have it look at the device you specified on the restore command line.

Non-Interactive Recovery

To recover all files from a dump, you would perform steps like the following:

```
cd /musr
restore rf /dev/st0
```

This will overwrite files in the target directory if they already exist.

Recovery from a Tar file

You can selectively recover files from a tar archive, or recover all files. Again, keep in mind that files could be overwritten and that they may be “busy” if in use. You may want to consider restoring the files to an intermediate location and then copying those you need into the target location.

Full restore using tar

In this example, we have a tar archive on the tape in */dev/st0* that contains a backup of */musr*. We wish to recover the entire contents.

```
cd /musr
tar xpf /dev/st0
```

Selective restore using tar

This example is similar to the full restore, but we wish to recover only certain directories from the archive. In this case, we will get the files for john and mary, but only the bin directory for mary.

```
cd /musr
tar xpf /dev/st0 mary/bin john
```

Restoring "/var", "/musr" "/nm" file systems

The NTM file system backup procedures recommend excluding directories to reduce backup errors.

If you have excluded directories from the backup list, verify and create the directories with the following permissions and ownership after completing the recovery process.

Important! After restoring **"/var", "/musr" "/nm"** file systems recreate the database by following Building the databases in the *Installation Guide*.

Table

Table 4 provides permissions, owner, and group for the files.

Table 4 Permissions, owner, and group for "/var" files

Permission Settings	Owner of File	Group	Filename
drwxr-xr-x	root	root	"/var/adm/crash"
drwxr-xr-x	root	sys	"/var/adm/sw/patch/tmp"
drwxrwxrwx	bin	bin	"/var/tmp"
drwxr-xr-x	bin	bin	"/var/opt/pd/tmp"
drwxrwxrwt	root	root	"/var/spool/cron/tmp"
drwxrwxrwx	bin	bin	"/var/dt/tmp"
drwxr-xr-x	nsadmin	nsgroup	"/nm/web/tmp"
drwxrwxrwx	nmadm	nm	"/musr/auds", "/musr/auds/rsp", "/musr/auds/tmp", "/musr/log", "/musr/meas"

□

Accessing arcmanager

Overview

Purpose

You can access the NTM `arcmanager` menu in two different ways:

1. logging into the system as `nmadm`
2. logging in to the system as `root`.

Contents

This section contains the following topics:

□

Accessing arcmanager — as “nmadm”

Instructions

Follow these steps to access the `arcmanager` menu using the `nmadm` login:

1 Log in as `nmadm`

2 Execute `/nm/ubin/arcmanager`

Result: The screen will show the following choices:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  7) Exit the backup program
```

END OF STEPS

□

Accessing the arcmanager -- as "root”

Instructions

Follow these steps to access the `arcmanager` menu using the `root` login:

1 Log in as `root`

2 Execute `/nm/ubin/arcmanager`

Result: The screen will show the following choices:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  6) Exit the backup program
```

END OF STEPS

□

Using arcmanager in non-interactive mode

Purpose

Arcmanager in non-interactive mode is meant to be used to automate backup tasks (i.e. from cron job or script). It provides limited functionality compared with arcmanager in interactive mode. Currently supports only creation of disk backups from historical area.

Syntax

Following syntax is used to create a disk backup:

```
arcmanager [-n name] [-d directory] backup disk [time]
```

Parameters

Archive name will be configurable with –n and -d options.

`name` Name for the backup file. The default is `nmYYYYMMDD` (where YYYY is year, MM – month, DD – day for specified date, e. g. nm200100820)

`directory` Directory for the backup file, default is configurable as HISTBACKUP in `arcmanager.conf` configuration file.

Important! Note that chosen directory needs to be accessible and writable by nmadm user.

`time` Optional parameter to specify which day from historical data to backup, default is 'yesterday'.

Hint: Execute info date for description of GNU date command and `--date` *option for information for possible values of time parameter.*

Errors

If run from cron it will suppress it's output to prevent receiving email from cron eigher on success or failure. An email will be sent on failure to MAILTO user (nmadm by default) defined in arcmanager.conf configuration file. The email notification feature can be disabled by specifying empty email address.

If arcmanager is run from a terminal window it will diplay the output to the user.

Eigher of theese two behaviours can be changed with appriopriate option: -q for quiet mode (will allways suppress the output) and -v for verbose mode (will allways display the output).

Error will also be logged in standard arcmanager logs. If a directory which would contain backup files already exists, it will result in an error.

Examples

The following example will backup previous day to disk to the HISTBACKUP directory and use default name for the archive:

```
arcmanager backup disk
```

An optional parameter can be given to specify which day should be backed up. It will be day number relative to present day. For example 0 will mean “today”, 1 “yesterday”, etc. Same syntax is used as for the --date switch of date command (e.g. “yesterday”, ‘today”, “1 day ago”, “2 days ago”).

```
arcmanager -n test_backup -d /tmp backup disk 1
arcmanager -d /histbackup backup disk '3 days ago'
arcmanager backup disk yesterday
arcmanager backup last-saturday
arcmanager -n nm20100708 -d /histbackup backup disk
```

□

Custom backup and restore utility options

Overview

Purpose

The following procedures explain how to: list the databases, restore archived data from tape or disk and purge data from the archives. You may find this utility useful when running backup procedures.

Contents

This section contains the following topics:

□

Purging archive data

Purpose

The arcmanager utility can be used to manage archive data. It allows you to store historical data in the archive and also to purge data from the archive area. Use the following procedure to remove data stored in the archive area.

Instructions

Follow these steps to purge data from the archive area:

1 Access the arcmanager menu using one of the methods in the "Accessing arcmanager" (p. 57).

Result: The screen will show the following choices:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  6) Exit the backup program
```

2 Enter 4 at the "`Enter Choice:`" prompt.

Result: The system responds with a list of archives available on the system.

3 Select the archive you wish to delete and press **ENTER.**

Important! Archived data is a segment of data selected at the time it was stored in the archive, therefore each archive can only be deleted in its entirety.

CAUTION

For archive purposes, each day ends at 12:00 midnight. If the archive you select to be purged was created as part of an archive

that spanned two days, deleting either part of the archive will result in the other part also being deleted.

END OF STEPS

□

Listing the databases

Purpose

Using the arcmanager utility you can determine which databases need to be, or have been backed up. If archive has been backed up, the last backup type and name will be displayed. It will also list the archives available on your system.

You can also run the `rdbstat` command from the *Linux* command line to display this information as well.

Instructions

Follow these steps to list the databases:

1 Access the "`arcmanager`" menu using one of the methods in the "Accessing arcmanager" (p. 57).

2 Enter `5` at the "`Enter Choice:`" prompt.

Result: The screen will show your system's databases and archives:

```
             List all available databases

Historical Databases:
        1) start:  06/13/2005-00:00  end:  06/13/2005-23:55
                DB was backed up on 06/14/2005-10:27 to disk as
   /nm/rdb/export/histbackup/nm20100613
        2) start:  06/14/2005-00:00  end:  06/14/2005-23:55
                DB was backed up on 06/15/2005-12:41 to archive as
   nm20100614
        3) start:  06/15/2005-00:00  end:  06/15/2005-23:55
               DB was backed up on 06/18/2005-11:03 to tape as nm20100615
     4) start:  06/16/2005-00:00  end:  06/16/2005-23:55
                DB has NOT been backed up
        5) start:  06/17/2005-00:00  end:  06/17/2005-23:55
                DB has NOT been backed up
        6) start:  06/18/2005-00:00  end:  06/18/2005-23:55
                DB has NOT been backed up
     7) start:  06/19/2005-00:00  end:  06/19/2005-23:55
                DB has NOT been backed up
        8) start:  06/20/2005-00:00  end:  06/20/2005-23:55
                DB has NOT been backed up

Archive Databases:
```

```
1)  NM20050527_0005__20050527_0025:  start:  05/27/2005-00:05  end:
   05/27/2005-00:25
2)  NM20050528_0005__20050528_0105:  start:  05/28/2005-00:05  end:
   05/28/2005-01:05
3)  NM20050530_0000__20050530_0005:  start:  05/30/2005-00:05  end:
   05/30/2005-00:05
4)  NM20050605_1000__20050605_1000:  start:  06/05/2005-10:00  end:
   06/05/2005-10:00
```

3 Press **ENTER**

END OF STEPS

□

Restoring archived data from tape

Purpose

An ***archive*** tape is one that contains periodic data from the NTM database. Archive tapes are used for analysis and troubleshooting, as well as for producing reports on network events.

> **Important!** You will not be able to access the database being used to load archived data while the data is being loaded. Any data in other databases (including the current database) is accessible.

Instructions

Follow these steps to load archive tapes for analysis:

1 If you want to restore the online database, log in as `nmadm`. Otherwise, proceed to Step 3.

2 Enter `stopsys`

3 Log in as `root` and access the "`arcmanager`" menu.

Reference: "Accessing arcmanager" (p. 57)

Result: The screen will show the following choices:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  6) Exit the backup program
```

4 At the "`Enter Choice`" prompt, enter `3` to restore data.

5 At the prompt, "`Restore data from tape or disk? [t,d]:`" Select "t" to restore data from tape.

Result: The system returns a prompt “`Select which device to use`”.

6 Enter a number, a name, or the initial part of a name, of the drive you wish to use for the restoration.

Hint: The name of the drive is dependent on the configuration at the customer site.

Result: The system responds with the prompt, “Load the tape onto tape drive <your drive>”. Press <RETURN> when ready.

7 After loading a tape in the drive you selected, select `return`

8 At the prompt, "`Restore data to Archive or Historical database? [a,h]:`"

Select "a" to restore data to the archive.

Select "h" to restore data to a historical database.

Important! You will not be allowed to overwrite historical databases on the NTM host. The "h" option is used to recover historical data after a system failure or corruption of a database on the NTM host.

Result: The system responds with: “`Output will be written to the Archive Log.” Should it be displayed here also? [y,n] (Default is y):`

9 Select `enter`.

Result: The system retrieves a list of previously stored data on the tape.

10 Verifying archive parameters. Please wait for further prompting
Restoring archive ID 'kbi0505_0800_0805' for - made on 05/06/2005-10:42
Estimated size of requested archive is 40 MB.
Current available space is 216401 MB
Do you wish to proceed? [y/n]:

11 Enter “y” to restore the data to the NTM host.

Result: The data from the archive is restored to the NTM host.

See Chapter 8, “Accessing Historical Data” in the *System Overview* for more information on loading archive tapes.

END OF STEPS

□

Restore archived data from disk

Purpose

A disk ***archive*** is one that contains periodic data from the NTM database. Disk archive are used for analysis and troubleshooting, as well as for producing reports on network events.

Important! You will not be able to access the database being used to load archived data while the data is being loaded. Any data in other databases (including the current database) is accessible.

Instructions

Follow these steps to load archive tapes for analysis:

1 If you want to restore the online database, log in as `nmadm`. Otherwise, proceed to Step 3.

2 Enter `stopsys`

3 Log in as `root` and access the "`arcmanager`" menu.

Reference: "Accessing arcmanager" (p. 57)

Result: The screen will show the following choices:

```
BACKUP AND RESTORE ROUTINES

  1) Save historical data
  2) Save archive data
  3) Restore data
  4) Purge archive data
  5) List the NM databases
  6) Exit the backup program
```

4 At the "`Enter Choice`" prompt, enter `3` to restore data.

5 At the prompt, "`Restore data from tape or disk? [t,d]:`" Select "d" to restore data from disk.

6 At the "`Enter the directory to search for backups [<HISTBACKUP direcotry>]:`" press ENTER to use default HISTBACKUP directory as location of disk backups. If you want to use custom location, enter full path to it and press ENTER.

Result: List of disk archives is displayed:

1) nm20100815

2) nm20100816

3) nm20100817

4) nm20100818

7 At the "`Enter archive number, or "q" to return to main menu:`" Provide number for selected disk backup and press ENTER.

8 At the prompt, "`Restore data to Archive or Historical database? [a,h]:`"

Select "a" to restore data to the archive.

Select "h" to restore data to a historical database.

Important! You will not be allowed to overwrite historical databases on the NTM host. The "h" option is used to recover historical data after a system failure or corruption of a database on the NTM host.

Result: The system responds with: "`Output will be written to the Archive Log." Should it be displayed here also? [y,n] (Default is y):`

9 Press `enter`.

Result: The system retrieves a list of previously stored data in the disk archive.

10 Verifying archive parameters. Please wait for further prompting
Restoring archive ID 'kbi0505_0800_0805' for - made on 05/06/2005-10:42
Estimated size of requested archive is 40 MB.
Current available space is 216401 MB
Do you wish to proceed? [y/n]:

11 Enter "y" to restore the data to the NTM host.

Result: The data from the archive is restored to the NTM host.

See Chapter 8, “Accessing Historical Data” in the *System Overview* for more information on loading archive tapes.

□

6 Generating a Crash Dump

Overview

Purpose

When an *HP-UX* system crashes, it saves a copy of the main memory (RAM), as it stands at the time of crash, along with other information in a sub-directory under the *"/var/adm/crash"* directory.

Recommended time allotment for procedure

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Analyzing a crash dump (preliminary)/making crash dump tape" (p. 3)	2 Hours	X	X

Contents

This chapter contains the following topic:

□

Analyzing a crash dump (preliminary)/making crash dump tape

Instructions

Follow these steps to perform a preliminary analysis of a crash dump and build a crash dump tape:

1 Log in to the machine as `root`.

Hint: You must know the `root` *password.*

2 At the shell prompt, type either of the following lines:

```
cd /var/adm/crash/core.0
cd /var/adm/crash/core.N
```

Result: This changes the current working directory to *“core.0”*, which is the directory where the core to be analyzed is present. If other core directory(s) (core.*N*) is (are) present, the latest core is the one corresponding to the greatest '*N*'. We recommend that you always select the latest core for analysis.

3 Verify the date stamp on the directory to ensure the crash dump is the latest one available.

4 Put a tape in the tape drive.

5 At the shell prompt, type:

```
find . | cpio -ocduvB > <tape drive>
```

Result: This copies the contents of the directory containing the crash dump to the tape.

Hint: Typically on a K-series machine the tape drive is: /dev/rmt/0m

6 When the shell prompt returns, remove and label the tape.

7 Contact Alcatel-Lucent Customer Support and make arrangements to send them the crash tape.

Result: Alcatel-Lucent Customer Support will analyze the problems and suggest a solution.

---

8 At the shell prompt, type

```
.  /usr/contrib/Q4/bin/set_env
```

Result: This sets the environment for the q4 tool.

---

9 At the shell prompt, type:

```
/usr/contrib/Q4/bin/q4pxdb ./vmunix
```

---

10 At the shell prompt, type:

```
/usr/contrib/Q4/bin/q4  -p  .
```

Hint: Note that there is a period in the above command.

Result: This starts the q4 test and returns a "`q4>`" prompt.

---

11 At the `q4` prompt, type:

```
run WhatHappened > wh.out
```

Hint: "wh.out" is an ASCII text file that can be useful in determining the cause of the crash.

---

12 At the `q4` prompt, type:

```
run Analyze AU > ana.out
```

Hint: "ana.out" is an ASCII text file that can be useful in determining the nature of the crash.

---

13 At the `q4` prompt, type `exit`

14 After the Alcatel-Lucent personnel have analyzed the problem and provided a solution, you may remove the directory that contained the crash dump.

END OF STEPS

□

7 Administrative Performance Reports

Overview

Purpose

This chapter discusses:

- Gathering of *Linux* system performance statistics with the *Linux* tools `sar`
- Using the Performance and Troubleshooting Reports (PATR) feature to collect and output application performance data

Contents

This chapter contains the following topics:

□

Linux system performance measurement tools

Overview

Linux ***system performance measurement tools*** analyze the behavior of the computer itself (hardware and software) independent of the actual work being performed.

There are many *Linux* operating system tools that gather system statistics. The system activity reporter (`sar`) is one such tool that provides system information.

Both the `sar` is automatically run by the system as part of cron. Information is gathered continuously and archived on a regular basis. The package features report commands that allow you to display readable information.

References

Because this is a *Linux* tool, it is fully documented in Linux user documentation and not in this guide. The information presented in this section is meant to be an overview and quick reference to using this tool, but is not intended to replace the official Linux user documentation.

□

SAR package

Overview

The sar daemons (collectors), which actually gather the system statistics, were configured prior to shipment of the NTM system.

The sar package provides low-level statistics of processor, memory, and device activity (disk and terminal).

Obtaining and interpreting a SAR report

To obtain a full sar report, enter the following command:

```
sar -A
```

References

For details about sar, see the *Linux* reference manuals.

□

Performance and Troubleshooting Reports feature (PATR)

Overview

The Performance and Troubleshooting Reports feature (PATR) enables NTM personnel to collect application performance data and output upon request. Depending upon the report type selected, the data may be real-time or hourly. The hourly data may be for a 24-hour period or less. Seven days of data are collected and stored for report access.

Information that can be output in reports includes counts of DCCs and switches in the NTM database; counts of DCCs and switches activated for data collection; counts of switches reporting/not reporting on time; counts of TGs and TGs reporting data; counts of TG calculations and threshold operations; TG total exceptions; etc.

PATR commands

One NTM command iseither input manually or scheduled by cron action to output the desired PATR report types. This commands are:

- `perfrep` — Use this command to output performance reports based on historical (not real-time) data saved in daily log files for a maximum of 7 days of data.

Permission to use the `perfrep` command is controlled by the *"/nm/etc/permissions"* file.

Data collection (perfcol process)

PATR data collection is performed by a new daemon process: ***perfcol***. This process is started in the */etc/inittab* file, so it is invoked whenever the host is booted. Counters and other data are retained after a reboot.

PATR log files — /musr/meas/log

The data used to generate the `perfrep` reports is stored in the directory *"/musr/meas/log"*. There will be a file for each day of data collected, with the naming convention "meas.MM.DD". A cron action deletes files as they age past 7 days, and the files should therefore not require maintenance. You can only generate perfrep reports for data contained in the log files.

You cannot read these data files.

□

The perfrep command

Format(s)

The format for the perfrep command follows:

```
perfrep [report=daily|summary|page] [date={1-12}/{1-31}]
   [starttime={0-23}] [endtime={0-23}]] [format=user|data] [-
   h]
```

Parameters

Through selection of the report= keyword, you can produce one of three report types:

- daily
- summary

The daily and summary report types provide exactly the same data, but the daily report provides a complete 24-hour period by hour, while the summary and page reports allow you to use the starttime and endtime arguments to limit report output to a particular interval of hours during the selected day.

The format= argument may be used to specify output in one of three forms:

- user — This causes data to be output in a standard report format suitable for reading or printing. This is the command default if the format= argument is not specified.
- data — This causes data to be output in a format suitable to be read into a spreadsheet or database to produce graphs, bar charts, and other types of graphic representations. The data is separated by comma delimiters.
- dcs — This format is no longer used and will not be discussed.

The -h argument provides a perfrep help message.

□

PERFREP reports — daily and summary

Overview

An example of a `perfrep` report (`report=daily`) is shown in Figure 1, “PERFREP command output where 'report=daily'” (p. 10). A `report=summary` version of the report contains exactly the same data in exactly the same sequence, but for a selected span of hours rather than a full 24 hours.

The report is printed to the screen or other output in three 8-hour segments. Only the first segment and the header of the second segment are shown in the figure.

Legend

The space immediately following a data field is reserved as a key field. This key field may be blank, indicating no problem, or contain these symbols:

- # Indicates “data is missing”
- * Indicates “data is suspect”

In the example report, which was taken from a laboratory test machine, no data is indicated as either missing or suspect.

Report output

The `perfrep` daily and summary reports provide hourly data on the following items:

- **DCCs Activated (Data Collection Concentrators)** — The number of DCCs activated is a count of the number of DCCs where data collection is activated for 5-minute ***measurements***. The count is therefore a reflection of the DCC status shown in the output of the `linkstat` command.
- **Switches Activated** — The number of switches activated is a count of the number of switches where data collection is activated for 5-minute ***measurements***. Similar data can be viewed using the `linkstat` command.
- **Reporting Ontime** — The number of switches reporting on-time is a count of the switches that reported their 5-minute measurement data within a time boundary set by the “/nm/db/dcoltimer” file for on-time data. Values in the file may vary from 90 to 230 seconds, using a procedure documented in the *System Overview*. If no file is

present, default is 100 seconds. This time boundary (usually referred to as "t1") is the point when the contents of shared memory are dumped to update the displays in autoupdate mode with exception data even if some switches have not yet reported.

If switch data is received after t1, but before a second timeout point "t2" (default 240 seconds), the data is stored in the current database, but the displays are not updated. This data is considered "late" (not on-time). Late data in the current database will be available for page retrievals and report output.

The period from t2 to 300 seconds (5 minutes) is a lockout period. Data received after t2 is not processed for exceptions and is not stored in the current database.

Optimally, the number of switches activated equals the number of switches reporting on time.

- **Reporting Late** — Switches that complete reporting after the `dcoltimer` "t1" time boundary are marked as reporting late. If all switches have not completed reporting before the `dcoltimer` value (or the default of 100 seconds), then an exc_late event occurs. The map displays indicate this condition by showing a box with an L. When a switch completes reporting but is late, this triggers an exc_more event. The map displays indicate this condition by showing a box with an R. This indicates that at least one late office has reported its data.
- **Not Responding** — The number of switches not responding is a count of switches that did not report measurement data at all or that reported data after the "drop dead" t2 timer mark of 240 seconds into the 300-second cycle. NTM reserves the time remaining after t2 but before the end of the collection cycle (300 seconds) to clean house in preparation for the next cycle. During this clean-up period, any late data coming in is ignored.
- **Trunk Groups Reporting Data** — The number of trunk groups reporting data is a subset of the number of trunk groups in the data base. Optimally, the number of trunk groups for which data is reported equals the number of trunk groups scheduled in the database and at the switch for data collection.
- **Num TG calcs (in K)** — On a 5-minute basis, the average number of calculations performed in thousands for the hour.

  Reference: See Chapter 10, "NTM Engineering Guidelines" in the *System Overview* for more information on the number of calculations allowed.
- **Trunk Groups in Exception** — On a 5-minute basis, the average number of trunk groups in exception for the hour. A trunk group is considered in exception when a calculation, count or flag exceeds the value indicated by the threshold index for the trunk group. See Chapter 10, "NTM Engineering Guidelines" in the *System Overview* for more information on the normal load of trunk group exceptions.

  When the number of exceptions exceeds these limits, the `limitthr` command can be run to reduce the number of trunk group and machine exceptions processed. The `limitthr` command does not affect exception processing of the GTD-5 PUP (peripheral unit processor) or HRLK (host remote link exceptions) measurements. If the system is operating at a heavy load level during normal operating periods, then the data should be checked to confirm that the exceptions recorded are meaningful. Some trunk groups may need to have thresholds updated in the ***thresh*** files or use another threshold index.

- **Machines in Exception** — On a 5-minute period basis, the average number of machines (switches) in exception for the hour. A machine is considered in exception when a calculation, count or flag exceeds the value indicated by the threshold for the count established in the office file.
- **TTO Exceptions** — On a 5-minute period basis, the average number of transmitter timeouts received for the hour.
- **Seconds Until Exception Update** — An exception update event is used to update the displays with the current data collected. Normally, an exception update (exc_upd) message is sent at the boundary set by the `dcoltimer`. Values less than the value of `dcoltimer` indicate that all switches have reported and exception processing was completed before the limit. Values greater than the value of `dcoltimer` indicate that exception processing is slow and the number of exceptions processed by the system should be checked.
- **Seconds Until Exception EOP (end of period)** — Data collection stops approximately 240 seconds after it starts, regardless of whether all switches have reported. This marks an exception end of period (exc_eop). Values less than 240 seconds indicate that all switches have reported and exception processing was completed before the limit. Values greater than 240 seconds indicate that data collection is slow. The number of late offices and offices not responding should be checked.

Capacity and usage reporting feature

Note that in Figure 1, “PERFREP command output where 'report=daily'” (p. 10), the report header labels the PATR report as the “Short-Format Daily Report for cbnmga on 01/16/96”. “cbnmga” is the name of a host NTM laboratory test machine. The reference to the report being “Short-Format” implies there must be a “long-format” version of performance reports, and there is. The feature is Feature 130, “Capacity and Usage Reporting” (CUR). PATR is provided with all NTM releases of 5.1 or higher. CUR is available only as a purchasable feature. The CUR feature provides all information contained in PATR, plus extensive and detailed additional results on data collection statistics, audit usage and performance, BDR (backup and disaster recovery) performance, database access performance, database maintenance activities, CPU use for data processing/access, system resources, etc. Chapter 14, “Capacity and Usage Reporting” provides detailed information on CUR.

□

Use of the PERFREP format=data argument

Overview

The previous report example was obtained by running the command `perfrep report=daily`. The argument `format=` was allowed to default to `format=user`.

If, however, you specify the argument `format=data` and direct the output to a file, that output can then be imported into an offline spreadsheet or database with graphing or other data manipulation capabilities. Comma delimiters are inserted between data items.

Figure 1 PERFREP command output where 'report=daily'

```
                                                                    Page  1
                        NTM Performance Report
                Short-Format Daily Report for cbnmga on 01/16/96

description             00:00  01:00  02:00  03:00  04:00  05:00  06:00  07:00
----------------------- ------ ------ ------ ------ ------ ------ ------ -----
Network Elements
  in Database

  DCCs activated            2      2      2      2      2      2      2      2
  switches activated       35     35     35     35     35     35     35     35
   reporting on-time       32     32     32     32     32     32     32     32
   reporting late           3      3      3      3      3      3      3      3
   not responding           0      0      0      0      0      0      0      0
  TGs reporting data       32     32     32     32     32     32     32     32

  num TG calcs (in K)       1      1      1      1      1      1      1      1

  TGs in exception         18     18     18     18     18     18     18     18
  Mach. in exception       29     29     29     29     29     29     29     29
  TTO exceptions           32     32     32     32     32     32     32     32

  Sec until excp upd       91     92     96     96     96     96     96     96
  Sec until excp EOP      158    160    164    164    165    164    163    163

LEGEND: # - data is missing             * - data is suspect
                                                                    Page  2
                        NTM Performance Report
                Short-Format Daily Report for cbnmga on 01/16/96


description             08:00  09:00  10:00  11:00  12:00  13:00  14:00  15:00
----------------------- ------ ------ ------ ------ ------ ------ ------ -----
Network Elements
```

```
in Database
            .
            .
            .
            .
```

□

8 Database Administration

Overview

Purpose

This chapter covers database administration. For disk layout see the "NTM Disk and File System Configuration" (p. 4) section of the *Installation Guide*.

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Building a new database (Tuxedo)" (p. 7)	15 Minutes	X	

Contents

This chapter contains the following topics:

□

NTM Databases

Overview

In NTM Release 15, two databases are used to support the system; a Tuxedo database and a relational database.

Tuxedo Database

A ***logical database*** consists of a TUXEDO database and *Linux* operating system file area. The *Linux* operating system file area corresponding to the offline database (nmdb0), online database (nmdb1), and each historical database (nmdb2-9) consists of those files stored in the directory *"/nm/unixdb/nmdb0-9"*. The periodic entity data is stored in the *"/rawdata"* filesystem under files associated with nmdb1-9.

The ***rawdata*** filesystem is used to contain the periodic raw data for the NTM online database and all the historical databases.

The RHEL platform provides eight historical databases. Each of these databases is identical in structure to the others and contains all the data from a single day (could actually be up to 25 hours).

Reference: Database ***cloning*** is:

- The duplication of a given database into another database.
- Done automatically by the dayend routines and by the `build_db` command.

Relational Database

The ***rdb1 and rdb2*** filesystems are used to contain the periodic raw data in a relational database format for the current and historical periods.

□

Database related processes

Overview

Databases are created at the time of system load and are accessed or maintained by the following processes:

Tuxedo only processes

- `build_db` (*"/nm/dbutil/build_db"*) — allows you to construct new databases. Normally used only in the process of loading the application tapes for a new system or a modified application issue
- `create` command — acts differently depending on file type object (single office or other). Tests, compiles, and moves single office files from the record base to the current database. Tests, compiles, and moves other files or all files to the temporary database.
- `dayend` routines — executed by cron action each night to copy the current database to the oldest historical database.
- `dbstat` command (Tuxedo databases only) — allows you to view the status of all Tuxedo databases and provides you with the following information regarding the Tuxedo database:
  - Database name
  - Database index
  - Raw devices used
  - Start and stop times for the database (data is stored in a database from the start time to the stop time)
  - Whether the database is active or out of service
  - Whether the database is on hold (removed from the historical database rotation pool)
  - Whether the database needs to be backed up
  - Whether the database is being used as the "current" or "off-line" database

  Important! One database should be marked as "offline" and one should be marked as "current". These two databases must always be active. If this is not the case with your system, contact customer support.
- `dbadmin` command (Tuxedo databases only) — allows you to change the status of a database. When using the `dbadmin` command to modify the database, you ***must*** log off, then log in for the system to make the status change.

Relational only processes

- `install_rdb` (*"/nm/rdb/dbinst/bin/install_rdb"*) (Relational databases only) — allows you to construct new relational databases. Normally used only in the process of loading the application tapes for a new system or a modified application issue.
- `rdbstat` command (Relational databases only) — allows you to view the status of all relational databases including those in the archive area.

Both Relational and Tuxedo related processes

- `installdb` command — allows you to move reference data from the temporary database (tmp db) into the current Tuxedo and relational databases.

⚠ **CAUTION**

Any attempt to modify these system files directly could result in loss or corruption of one or more databases.

□

Current, offline, and dayend manipulation (Tuxedo)

Overview

One database is always designated “offline” and one “current”. The remaining databases are part of the historical database pool.

The offline database is used by the `create` command. The `create` command compiles the user record base files (*“/musr/rb”*) and loads them in the offline area.

The `installdb` command copies all or part of the offline database to the “current” database.

The current database holds the most recent 25 hours of data. This is the area into which the results of ongoing data collection, exception calculation, and control activity are stored.

At the end of each day (the actual time can be set by the user in a crontab file), the “current” database is copied to the oldest active database not in the “hold” state. This database then becomes the “historical” database. This is the `dayend` routine.

If you have also scheduled a dayend `installdb`, it is performed at this time and the audits are automatically run.

References

“create” (p. 5) and “installdb” (p. 34) in the *Input Commands Guide*; “Performing a full create and installdb” (p. 3) in the *Record Base Administration Guide*

□

Building a new database (Tuxedo)

Purpose

It may be necessary to build (or rebuild) the NTM database when loading the system or during some emergency situations. This procedure takes around 15 minutes to complete.

CAUTION

This procedure will destroy the contents of the existing databases.

CAUTION

If you have BDR, deactivate it during this procedure or you will damage your database.

Instructions

Follow these steps to build a new database:

1. Enter `stopsys` to stop the system.

2. Log in as `nmadm`

3. If you have BDR enter `/nm/sys/bdr_deact` to deactivate BDR.

4. Enter `/nm/dbutil/build_db` to build the new databases.

5. If you have BDR, enter `/nm/sys/bdr_act` to activate BDR.

□

9 Adding and Removing Network Elements

Overview

Purpose

This chapter discusses how to add and remove network elements. The primary method for connecting network elements to the NTM host is through TCP/IP connections.

DCC migration

During the migration away from DCC's and to connect network elements to the NTM host directly through TCP/IP, we have included a section for "Migrating to TCP/IP connectivity" (p. 39).

Before you begin

If the system does not have *4ESS* switches, you must make the following change in "/nm/ubin/start.all" before running DCOL_4E. This change prevents the system from trying to collect *4ESS* entity information.

Change the line:

```
DCOL0:0:0:respawn:export SRVID=20;DCOL_4E -s
   DCAUDSVC0,DCADMSVC0,DCCTRLSVC0 -o /dev/null -e /dev/null -- -i 0
```

to:

```
DCOL0:0:0:respawn:export NO4ESS=1; export SRVID=20; DCOL_4E -s
   DCAUDSVC0,DCADMSVC0,DCCTRLSVC0 -o /dev/null -e /dev/null -- -i 0
```

Contents

This chapter contains the following components:

□

Time recommendations

Table

Table 1 lists estimated times to perform each procedure.

Table 1 Recommended time allotment for procedures

Procedure	Approximate Time Required
DCC	
Creating the record base files (DCC)	15 minutes
Installing the updated record base (DCC)	20 minutes
Performing post-DCC move steps on NTM	30 minutes
Performing post-DCC move steps on the EADAS	30 minutes
Removing the record base files (DCC)	15 minutes
Setting up the TCIP/IP link between the host and switch	1 hour
OFFICE (Non-4ESS)	
Creating the record base files (office)	15 minutes
Removing the record base files (office)	15 minutes
Updating the system after removing an office	90 minutes
Migrating to TCP/IP connectivity	1 hour
Setting up the infrastructure	1 hour
Preparing the non-NTM features	1 hour
Preparing the NTM host	3 hours
Cutting over an office	10–60 minutes
Backing out an office cutover	15 minutes
Verifying cutovers	10–30 minutes
Finalize cutovers and deactivate the DCC interface	1 hour

□

TCP/IP interface to a DCC

Overview

Purpose

This section discusses procedural and supporting information for DCCs.

Contents

This section contains the following components:

□

Requirements

Prerequisit features

The following FEP releases are supported with Feature 124, “TCP/IP Interface to FEP”: FEP (Release 2) and later

The following TDMS release is supported with Feature 245, “TCP/IP Interface to TDM”:TDMS Release 3.1 and later

The following NPM release is supported with Feature 369, “TCP/IP Interface to NPM”: NPM Release 6.0 and later

Coordination

It is necessary to coordinate use of this feature with record base personnel, as a change must be made to the record base “Office” file. A dialstring must be added for the TCP/IP connection.

Reference: “Required entries in the “/etc/hosts” file” (p. 6)

Required entries in the “/etc/hosts” file

Each DCC that will interface to an NTM using the TCP/IP interface must have an entry in the “/etc/hosts” file. Likewise, an entry must exist in the hosts file on the DCC that defines the host name and IP address of each NTM that it will interface to.

Here is an example NTM “host” file.

Figure 1 NTM “/etc/hosts” File

```
192.7.41.82     ntmos1 “optional alias”
192.7.41.82     ntmos2 “optional alias”
192.7.41.82     fepone "optional alias"
192.7.41.82     tdms1 "optional alias"
```

Reference: Sets File in the *Record Base Administration Guide*

Communicating with DCCs over the TCP/IP network

Ethernet interface connections between NTM and a DCC must exist. Additionally, network route(s) must exist so that the systems can communicate with each other.

Depending on the method of implementation, static or dynamic routing can be established.

NTM to DCC communications using TCP/IP may share the same Ethernet interface on the system that is used for normal data traffic to the host NTM machine.

□

Specifying a new far end destination remote host to the TCP/IP protocol database

System administration personnel are responsible for modifying the TCP/IP host and routing data.

This TCP/IP data exists on the NTM systems for other system functions (for example, rlogin, ftp, telnet...); however, the WAN that these functions use may not contain a route to the required switching system. In addition, even if the WAN supports basic transfers of data between NTM and the switch, there exists the strong possibility that the route taken by the data to/from the far end is insufficient in one or more of the following ways:

- Number of hops (physical path); could cause delays in data delivery
- Quality of service (will the data arrive in a timely manner)
- Bandwidth (size of the data pipe); this issue occurs when NTM must compete on the same LAN/WAN with other normal business functions. It is STRONGLY recommended that NTM **NOT** be provisioned on the same physical LAN that carries “regular business” functions. The practice of assigning realtime communication traffic to business LANs has been known to cause multiple anomalies in network systems.
- Hardware configuration; failure of a single hardware unit could cause an NTM outage to certain switches (or groups of switches, or ALL switches in the worst case scenario). There should be planned hardware redundancy in the case of ALL interfaces that route to target switches. This affects all hardware on path to the far end: Network Interface Cards (NICs), routers, physical connections. In the ideal case NTM would use two different physically diverse paths on two separate interfaces to one target switch (for example, one path via land-line, the other via microwave channel).
- WAN/LAN carrier; the method and size of the pipe that connects NTM to the far end switch must be considered. The delivery of TCP/IP data will be adversely affected if the carrier is not sized properly or is not of a high quality.

Adding routing data

It is necessary to add routing data for each switch from which NTM will collect data. This is accomplished by the system administrator (requires root privilege) in one of several methods outlined in the RHEL manual.

The simplest method is to simply add an entry in the “/etc/hosts” file on NTM for each target switch specifying the CLLI (Common Language Location Identifier) that NTM recognizes.

This “/etc/hosts” file entry is of the form:

```
# The form for each entry is:
# <internet address> <official hostname> <aliases>
     130.88.47.172       switch_name     possible_switch_alias
```

This method is only one of several methods used to determine how the switch CLLI is translated to the proper interface for TCP/IP communication. Other methods, Domain Name Service (DNS) and Network Information Service (NIS/BIND), accomplish the resolution of the switch CLLI to TCP/IP address. These methods are specified in the appropriate RHEL documents. You must add the name resolution capability for each and every data collection switch.

The "/etc/nsswitch.conf" file determines the method used to perform the CLLI to IP address translation: Linux files database, Domain Name Service (DNS) or Network Information Service (NIS). From "/etc/nsswitch.conf" the system will find the translation method.

The "/etc/nsswitch.conf" file possibly needs to be modified to reflect the method chosen to resolve a CLLI to an IP address. If the basic Linux file method is chosen then the file would look like the following example file, "/etc/nsswitch.files":

```
passwd:       files
group:        files
hosts:        files
services:     files
networks:     files
protocols:    files
rpc:          files
publickey:    files
netgroup:     files
automount:    files
aliases:      files
```

Also, if an implicit route to the far end switch is not available through the "default" route then an explicit route must be added so that the IP protocol knows how to reach the far end. This can be accomplished using the following methods:

- manually using the /usr/sbin/route command (refer to the "route(1M)" command in your *Linux* operating system documentation or use the online `man` <*command_name*> command.)

Operating system checks

The condition of the route/path to the far end of a TCP/IP link may be determined using a few *Linux* commands: /usr/sbin/ping, /bin/telnet, /usr/contrib/bin/traceroute. First try using ping specifying the CLLI or IP address of the target switch. If the after a length of time (thirty seconds) the control-C key combination (*Linux* INTR signal) will display the packet loss statistics. If the packet loss statistics are greater than approximately ten percent (10%) then a problem exists in the route chosen to reach the far end.

□

Using and testing TCP/IP connections

Before you begin

Prior to activating a new DCC on NTM, verify that the communications path is available between NTM and the DCC.

> **Important!** It is not recommended that a DCC be left active for extended periods of time on NTM if the communications path is not operational. This causes many connection attempts and messages to be logged in the "/musr/log/errors" file.

Operating system checks

There are commands provided as part of the *Linux* operating system that may be used to verify the communications and status of the network. Refer to the "ping", "telnet", and "netstat" commands in your *Linux* operating system documentation, or use the online `man` <*`command_name`*> command, to obtain more information about these commands.

"Ping" is a command that can help determine how far down the communications path a signal is getting. It can be used to send a message for basic loopback to the sending hosts or can be targeted to any intermediate point in the route if the "host name" or "IP address" is known. Ultimately, a "ping" should execute end-to-end.

Application checks

The NTM application code contains a command that may be used to send a test message to the DCC.

> **Reference:** "sendmsg" (p. 20) in the *Input Commands Guide*.

Once the communications path has been verified and all the necessary administration work in both NTM and the DCC has been completed, the link can be activated. The log files and the `linkstat` command may be used to determine the status of the link. Also, the `linkstat` command output shows which interface is active to the FEP or TDMS.

> **Reference:** "linkstat" (p. 9) in the *Input Commands Guide*.

Communications link

The *Linux* "netstat" command can be useful in determining the amount of traffic, routing table information, and certain network conditions, such as packets rejects, etc.

Refer to the "netstat" command in your *Linux* operating system documentation, or use the `man` <*`command_name`*> command, to obtain more information about the "netstat" command.

Routing table changes

The *Linux* “route” command can be used to update the routing table.

Refer to the “route” command in your *Linux* operating system documentation, or use the online `man` <*`command_name`*> command, to obtain more information about the “route” command.

Network bandwidth

As with any network, successful transmission and effective communications are dependent on appropriate bandwidth being available. Obviously, with a network traffic management system it is very important that the bandwidth be adequate for busy periods as well as for typical loads.

□

Adding a DCC

Overview

Purpose

This section provides procedures and related information to add a new DCC to be controlled by NTM. To add a new DCC to be controlled by NTM, you must create the record base files for the new network element and then install the updated record base.

Contents

This section contains the following components:

□

Creating the record base files (DCC)

Instructions

Follow these steps to create the record base files:

1 Establish links to the DCC.

2 Add the DCC to the RSPTE File.

Reference: "RSPTE File" (p. 68) in the *Record Base Administration Guide* explains how to add the DCC to this file.

3 Add an Office File for the DCC.

Reference: "Office File" (p. 40) in the *Record Base Administration Guide* explains how to add an office file.

4 Enter `dbtest` to check the RSPTE File for errors.

END OF STEPS

□

Installing the updated record base (DCC)

Instructions

Follow these steps to install the updated record base files:

1. Enter `create rspte` to create the RSPTE File.

   Reference: See Chapter 7, “Record Base Administration” in the *Record Base Administration Guide*.

2. Enter `stopsys` to stop the system.

3. Enter `installdb rspte now` to install the updated RSPTE DCC entry in the current database.

4. Enter `dbtest` to check the DCC office file for errors.

5. Enter `create all` to create the new DCC office file entry.

6. Enter `startsys` to start the system.

7. Enter `act` to activate the DCC.

END OF STEPS

References

See the *Input Commands Guide* for information on each of these commands.

□

Structure: DCC office list

Overview

When the connection to a DCC is established, the DCC sends NTM a list of offices to which it is connected. NTM uses this list to determine which offices it may communicate with through that particular DCC. NTM can also request this list if an active DCC requests it.

> **Important!** Individual switch offices (entities) must be activated at the DCC to enable NTM to collect data for the offices from the DCC. Refer to the Front-End Processor (FEP) Administration Guide for information on activating FEP entities.

Output

The DCC output (list of connected offices) is written to the "/musr/ofclst" directory. There is a file for each DCC in this directory where the name of the file is the name of the DCC. In this file, a CLLI may be alias to another CLLI name. The format of the file is shown in Figure 2.

Figure 2 DCC File example

```
clli =  hrclca11ds0, type = DMS100, channel =  0
clli =  igncca1288l, type =  1AESS, channel =  1
clli =  labtolab5eh, type =   ESS5, channel =  2
clli =  lrksca11ds0, type = DMS100, channel =  3
clli =  lsbnca12ds0, type =   ESS5, channel =  4
clli =  mlbrca11ds0, type =   ESS5, channel =  5
clli =  nhldca11ds0, type =   ESS5, channel =  6
clli =  nlmtest1111, type = DMS100, channel =  7
clli =  npvlrs07e5h, type =   ESS5, channel =  8
clli =  nvcyca11ds0, type = DMS100, channel =  9
clli =  okdlca1184e, type =   ESS5, channel = 10
clli =  okldca03ds2, type = DMS100, channel = 11
clli =  okldca04ds0, type = DMS100, channel = 12
clli =  ptvlca1178e, type = DMS100, channel = 13
clli =  washdcut11t, type =   ESS5, channel = 14
clli =  nycmnyby01t, type =   ESS5, channel = 15
clli =  boston5esst, type =   ESS5, channel = 16
clli =  wtvlmeap02t, type =   ESS5, channel = 17
clli =  brtnmaco03t, type = DMS100, channel = 18
clli =  glflnygfds0, type =   ESS5, channel = 19  * NOT IN NM DATABASE *
clli =  dovrnhth02t, type = DMS100, channel = 20
```

In Figure 2

- "clli" is the name of the offices on the DCC

- “type” is the switch type
- “channel” is the DCC channel number
- The last field indicates those switches that are not in the NTM database or are offline at the FEP.

  Reference: Chapter 4, “Data Collection Concentrator Alias File” in the *Record Base Administration Guide*

□

Moving a switch to a new DCC

Overview

Purpose

Several procedures are required to make sure NTM and the DCC know that an office has been added or removed.

Contents

This section contains the following components:

□

Performing post-DCC move steps on NTM

Instructions

Follow these steps on the NTM:

1 Make sure the DCC procedure for building an office is followed in the DCC to which the office was moved and that the proper procedure is followed in the DCC from which the office was moved.

2 If the name of the office used in the DCC is different from that used in NTM, make an entry in the "/musr/rb/dcc_alias" file.

3 If the office's entry does not exist in the "/musr/rb/dcc_alias" file, then add it to that file.

4 Make sure you follow the DCC procedure for building an office.

5 Deactivate and activate the affected DCCs to move the office from the old interface data collector.

> **Reference:** See the deact_dcc command (7-13) and the act_dcc command (7-7) in the *Input Commands Guide*.

6 Enter `linkstat type=dcc`. Make sure that the DCC to which the office is connected is active and collecting information.

7 Execute `linkstat` on the office that was moved. Make sure that it is associated with the new DCC.

END OF STEPS

□

Performing post-DCC move steps on the EADAS

Instructions

Follow these steps on the EADAS:

On the EADAS *FROM* which the switch was moved:

1 Deactivate the entity.

2 Edit the entities file (under “/eusr/na/entity/rbasexx/entities/xxxx”) and change the “`nm enabled`” parameter from “yes” to “no.”

3 Execute `ice compile` on the entity.

4 Activate the entity (in order to get the change into DCC memory).

5 Deactivate the entity.

TO

6 Deactivate the entity (if already active).

7 Edit the entity file and change the “`nm enabled`” parameter from “no” to “yes.”

8 Execute `ice compile` on the entity.

9 Activate the entity.

END OF STEPS

□

Removing a DCC

Overview

Purpose

When removing a DCC from NTM's control, you must remove the record base files for the DCC and then install the updated record base. These procedures show the required steps and provide references to more detailed information.

Contents

This section contains the following components:

□

Removing the record base files (DCC)

Instructions

Follow these steps to remove the record base files:

1 Remove all switches from the DCC.

Reference: “Adding or removing an office” (p. 33)

2 Enter `deact` to deactivate the DCC for collection of measurements, audits, controls, and discretes.

3 Remove the DCC from the RSPTE File.

Reference: “RSPTE File” (p. 68) in the *Record Base Administration Guide*

4 Remove the Office File for the DCC.

Reference: “Office File” (p. 40) in the *Record Base Administration Guide*

END OF STEPS

□

Updating the system after removing a DCC

Instructions

Follow these steps to remove the record base files:

1 Enter `create all` to copy the record base files to the offline database.

2 Enter `stopsys` to stop the system.

3 Enter `installdb all now` to install the offline database into the current database.

4 Enter `startsys` to start the system.

END OF STEPS

References

Chapter 7, “Record Base Administration” in the *Record Base Administration Guide*

□

TCP/IP interface to offices

Overview

Purpose

This section explains the TCP/IP (Transmission Control Protocol/Internet Protocol) interface to the offices.

Background

The customer may select the direct-connect TCP/IP interface to the switch, or the previously existing DCC interface to the switch, when both exist.

It is necessary to coordinate use of this feature with record base personnel, as a change must be made to the record base Office File and RSPTE File for this feature to function properly. This includes adding a dialstring to the "Office" file for the TCP/IP connection, entering security settings in the "Office" file, and setting the "direct" connection option in the "RSPTE" file.

Contents

This section contains the following components:

□

Requirements

Equipment

TCP/IP Interface to the Switch requires the following:

- A properly equipped and engineered Ethernet between the NTM Feature Set and the Switch(es) from which data is to be collected
- The DMS 100/200 Switch must be equipped with a Supernode Data Manager loaded with a compatible TCP/IP and Ethernet protocol "stack"
- A properly configured security environment

Prerequisite features

This section applies when you are establishing a TCP/IP link to offices. Connections to SCSNSN (generic sn02 and later) type can only be made by directly connecting them to the NTM hosts via TCP/IP.

The TCP/IP Interface to offices prior to Release 13 was optional. Now it is required and is available through these features:

- DMS 100/200 Switches Generic NA013 and later only if Feature 277, "TCP/IP Interface to DMS 100/200 Switches" has been purchased.
- DMS 250 Switches Generic UCS13 and later only if Feature 293, "TCP/IP Interface to DMS 250 Switches" has been purchased. This feature expands from 200 to 800 simultaneous direct connect TCP/IP connections to switches from NTM. It is recommended the TCP/IP network used should be dedicated to the direct connect interfaces of NTM to avoid performance problems.
- DMS 500 Switches Generic NCS13 and later only if Feature 296, "TCP/IP Interface to DMS 500 Switches" has been purchased.
- *5ESS* Switches 5E15 Generic and later only if Feature 282, "TCP/IP Interface to 5ESS 5E15 Generic switches" has been purchased.
- Feature 381, "TCP/IP Interface to GTD-5 Switches"
- Feature 394, "TCP/IP Interface to 4ESS Switches via Datatek DT-4180"
- Feature 431, "TCP/IP Interface to 4ESS Switches via AI Switch"
- Feature 409, "TCP/IP Interface to 5ESS Switches via AI"
- Feature 410, "TCP/IP Interface to DMS Switches via AI"

Troubleshooting

In the event that all NTM data for a DMS switch being sent through a TDMS/FEP is missing at NTM, you will need to contact TDMS/NetMinder Customer Support for assistance.

The *DMS* switch can receive polls using either the EADAS interface (supporting up to 250 TGs) or the newer NTM interface (supporting up to 1024 TGs.)

One possible scenario is that NTM and the *DMS* switch are set up for 1024 TG support, but TDMS/FEP is not. In this case, TDMS/FEP will send polls for all NTM data for a given *DMS* switch along the EADAS interface, while the switch expects NTM polls only along the NTM interface.

Such a condition will result in no NTM data for this switch being sent to NTM. In this case, TDMS/FEP should be reconfigured to send NTM polls along the NTM interface.

If there is trouble connecting to the network element, verify port availability on the networl element using the netstat command.

Examples might be:

5ESS

```
“netstat -an | grep 60005"
```

DMS

```
“netstat -an | grep 9553"
“netstat -an | grep 9554"
“netstat -an | grep 9555"
```

□

Setting up the TCIP/IP link between the host and switch

Purpose

This procedure establishes the TCIP/IP link between the host and the DMS 100/200, DMS 250, DMS 500, *5ESS,* SCSNSN, Sonus GSX, and Sonus PLXswitch.

Instructions

Follow these steps to set up the link:

1 Create the link on the NTM host machine:

1. Enter `tcp` at end of entry for the value of the `direct` parameter for switch in RSPTE File.
2. Create the RSPTE File (`create rspte`).
3. Enter `stopsys`.
4. Install the RSPTE file (`installdb rspte`).
5. Enter `startsys`.
6. Deactivate the office if it is activated (`deact`).
7. Modify the Office File:
   - If establishing a link to DMS or SCSN office, add values for all three `dialstring` parameters and the `authentication` parameter.
   - If establishing a link to *5ESS* or 7R/E office, add values for the `dialstring` and `cpnode` parameters. Add an entry for the parameters in the PAS Code File.
8. Create the office (`create` office).
9. Add the clliname and the IP address of the office to the "etc/hosts" file.

   Important! If you have purchased the Backup and Disaster Recovery Features, this step will need to be done on each host.
10. Activate the office (`act`).
11. Enter `audit all`
12. Verify data collection from the office.

2 Contact switch personnel to activate their features that correspond to Feature 277, 282, 293, or 296 on the switch itself.

3 Activate the switch.

END OF STEPS

References

“Office File” (p. 40), “PAS Code File” (p. 64), and “RSPTE File” (p. 68) in the *Record Base Administration Guide*

See the related commands in the *Input Commands Guide*.

□

Adding or removing an office

Overview

Purpose

To add an office which is to be controlled by NTM, you must create the record base files for the new office and then install the updated record base.

> **Important!** DCC’s such as FEPs, TDMs, etc. and Protocol converters (Datatek 4180) should be configured before adding offices.

When removing an office from NTM's control, you must remove the record base files for the network element and then install the updated record base.

Contents

This section contains the following components:

□

Creating the record base files (office)

Instructions

Follow these steps to create the record base files:

1. Add the office to the RSPTE File.

2. Enter `dbtest rspte` to check this file for errors.

3. Enter `create rspte` to update the offline database.

4. If you have Feature 41, "Install RSPTE Without Stopsys", continue with Step 6.

5. If you do not have Feature 41, "Install RSPTE Without Stopsys":
   - Enter `stopsys` to stop the system.
   - Enter `installdb rspte` to move the newly built database from the offline area to the current area.
   - Enter `startsys` to start the system.

6. Add an Office File for the switch.

7. Add an Office Domain File for the office if you are adding a *4ESS*, *5ESS*, or 7R/E switch.

8. Add a Trunk Group File for the office.

9. Enter `dbtest office <office_name>` to check the record base files for errors.

10. Enter `create office <office_name>` to update the offline database.

11 Enter `stopsys` to stop the system.

12 Enter `startsys` to start the system.

13 Enter `act` `<`*`office_name`*`>` to activate the office.

14 Enter `audit` `<`*`office name`*`>` `all`

END OF STEPS

References

Chapter 7, "Record Base Administration" in the *Record Base Administration Guide*

□

Removing the record base files (office)

Instructions

Follow these steps to remove the record base files for an office:

1 Remove all active controls from the office, including any manual HTR (Hard-To-Reach) codes.

2 Enter `purglog` to remove all matched entries from the database for all switches.

3 Enter `deact <office name> all` to deactivate the switch for data collection.

4 Remove the office from the RSPTE File.

> **Important!** This step can only be done if all other references to this CLLI code are removed throughout the NTM record base.

5 Remove the Office File for the office.

6 Remove the Office Domain File for the office if you are removing a *4ESS*, *5ESS*, or 7R/E office.

7 Remove the Trunk Group File for the office.

8 Enter `dbtest all` to check the record base files for errors.

END OF STEPS

□

Updating the system after removing an office

Purpose

Once the office's record base files have been removed, you must update the current database.

Instructions

Follow these steps to update the system:

1. Enter `create all` to update the offline database for all record base file types.

2. Enter `stopsys` to stop the system.

3. Enter `installdb all now` to install reference data.

4. Enter `startsys` to start the system.

END OF STEPS

□

Migrating to TCP/IP connectivity

Overview

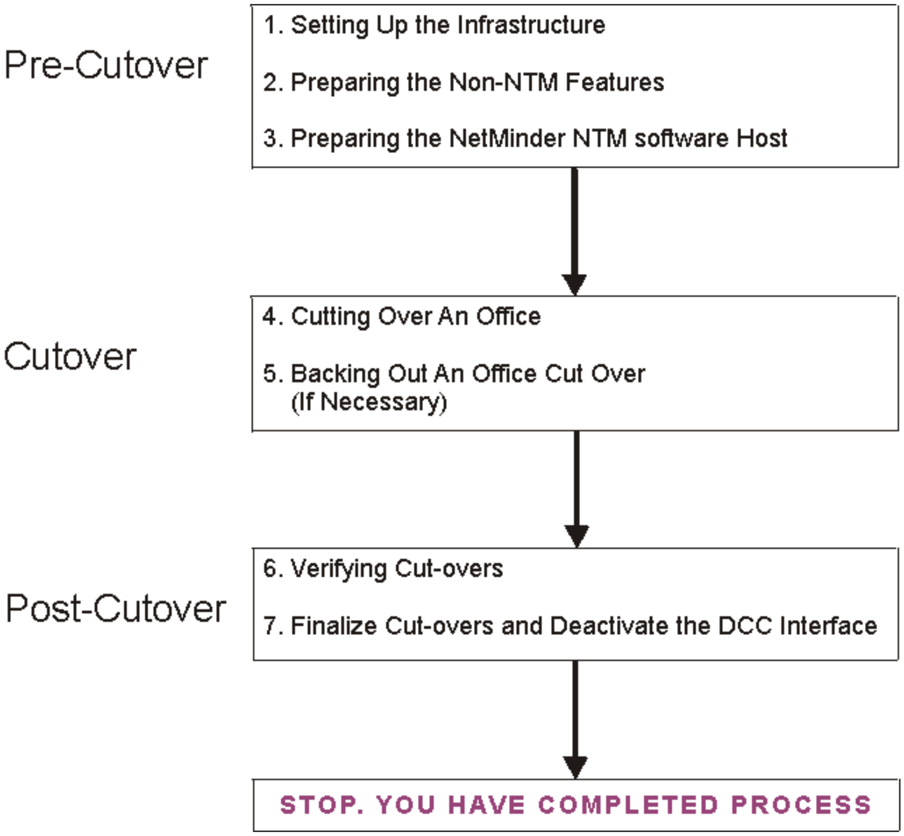
Purpose

This section describes the steps required to convert the NTM system to communicate with a *5ESS* or *DMS* office via TCP/IP.

Figure

Figure 3 provides a flowchart of the migration process.

Figure 3 Migration process


Pre-Cutover
1. Setting Up the Infrastructure
2. Preparing the Non-NTM Features
3. Preparing the NetMinder NTM software Host
Cutover
4. Cutting Over An Office
5. Backing Out An Office Cut Over (If Necessary)
Post-Cutover
6. Verifying Cut-overs
7. Finalize Cut-overs and Deactivate the DCC Interface
STOP. YOU HAVE COMPLETED PROCESS

Contents

This section contains the following components:

□

Time recommendations

Table

Table 2 lists estimated times to perform each procedure.

Table 2 Migrating to TCP/IP connectivity

Procedure	Approximate Time Required	Disrupt NTM Activities?
Setting up the infrastructure	1 hour	No
Preparing the non-NTM features	1 hour	No
Preparing the NTM host	1 hour	No
Preparing the NTM host for migration to AI	1 hour	No
Cutting over an office	3 hours	Yes
Backing out an office cutover	10–60 minutes	Yes
Verifying cutovers	15 minutes	No
Finalize cutovers and deactivate the DCC interface	10–30 minutes	No

□

Setting up the infrastructure

Instructions

Follow these steps to set up the infrastructure:

1 Update the “/etc/hosts” file on the NTM host with new IP addresses of the office, using the format:

```
XXX.XXX.XXX.XXX office_name
```

2 For *5ESS*, 7R/E, and *GTD-5* offices, update the Password File on the NTM host with an ID and password for each office.

3 Verify that “/etc/nsswitch.conf” file on the NTM host is defined properly. The “hosts” line should indicate that “files” are first as opposed to “dns”.

4 Verify TCP/IP protocol and Ethernet stack compatibility between the NTM host and the offices.

Between each office and the NTM host, execute:

```
ping
```

END OF STEPS

□

Preparing the non-NTM features

Time synchronization

It is highly recommended that the network have a solution for time synchronization available, as the DCC/FEP will no longer be able to mask time differences between the switches and the NTM host. All switches have a lockout period during which no NTM requests will be received. Synchronization is required to ensure that the NTM requests occur on or after the five-minute boundary for data collection. NTM has some tolerance for time differences (3-10 seconds depending on switch type) and will repoll if blocked, but data may be marked late or suspect in those cases.

The HP's operating system (HP-UX) supports an ntp-based time synchronization package. It requires the IP address of the machine to be used as the master time source. If no time synchronization is established, it will be the Customer's responsibility to keep the switches in sync with the NTM host.

Reference: "Time synchronization — 4ESS" (p. 3) in the *System Administration Guide*

Checklist

The Office Administrators must prepare each office to support the new TCP/IP interface.

Network Element	Ensure that each network element ...
5ESS	• is equipped with Administrative Services Module (ASM) • has the correct feature package (ASM feature 99-5E-7133) installed and configured The office administrator must supply: – IP address for ASM module – Username and password for NTM port (60005) (established on the ASM via the addnusr command) • has networking addresses in place • loaded with at least the 5e15 generic
DMS	• is equipped with the Supernode Data Manager (SDM) • has the correct feature packages installed and configured (including the SDM/SNM feature NMDC001) • has networking addresses in place • is loaded with at least the ucs13 generic.

Network Element	**Ensure that each network element ...**
GTD-5	• is loaded with at least the gtd4003 generic.

The DCC Administrator must be prepared to remove entities to no longer have the data forwarded to NTM.

For the new TCP/IP interface via AI switch the Office Administrators must prepare the following tasks.

Network Element	**Ensure that each network element ...**
5ESS	• is connected with properly configured AI Switch • has networking addresses in place • is loaded with at least the 5e4 generic
DMS	• is connected with properly configured AI Switch • has networking addresses in place • has loaded generic with at least the DMS24, UCS07 and NCS06 for DMS, DMS 250 and DMS 500 respectively.

Reference: Installing and Configuring AI Switch in the *Installation Guide*

References

Refer to the following documents regarding this feature on the *5ESS*/ASM.

- "*5ESS* Switch OneLink Manager Administrative Services Module User's Guide, ASM Release 6.0 or earlier", Document Number 235-200-145, Issue 3.00A, August 2002. Section 8.12 (starting on page 8-38)
- "7R/E *5ESS* Switch Local and Toll System Features, Feature Document, 5E13 and Later Software Releases", Document Number 235-190-115, Issue 10.00, November 2000. Section 12.4 (starting on page 12-13)

Supporting 1024 trunk groups involves adding hardware to the DMS and configuring it for the correct NTM ports (9553, 9554, 9555). Customers should review this "growth procedure" from Nortel before implementing that upgrade.

□

Preparing the NTM host

Instructions

Prepare the NTM host for the conversion by:

- Collecting information required from the office
- Networking Setup (define switches in "/etc/hosts", check "/etc/nsswitch.conf")
- Record Base Changes

1 Make sure that both the network element and the NTM host recognize each others IP addresses. For the NTM hosts, this can be done through the "/ets/hosts" file.

2 Edit the "/nm/ubin/start.all" file.

If this is a change from a data collector to TCP/IP and ALL offices are moved off the old DCOLs, please turn off the DCOLs for the data collector after moving the offices to the TCP/IP DCOLs.

Change "`off`" to "`respawn`" for the DCOL_<*`office type`*>

Default DCOL's are; 10 for *DMS* and 8 for *5ESS*

Example for a DMS:

```
DCOL10:0:0:respawn:export SRVID=30;DCOL_DMS -s
   DCAUDSVC10,DCADMSVC10,DCCTRLSVC10 -o /dev/null -e /dev/null
   -- -i 10
```

Example for a 5ESS:

```
DCOL8:0:0:respawn:export SRVID=28;DCOL_5E -s
   DCAUDSVC8,DCADMSVC8,DCCTRLSVC8 -o /dev/null -e /dev/null --
   -i
```

3 In case the cutover needs to be backed out, save a copy of the original files for the:

- Office File
- RSPTE File
- Password File (*5ESS,* 7R/E, *GTD-5*)

4 Update the office file for each office to be converted by replacing the "`;`" after `packets=all` with a "`,`" and inserting the following lines after the "`packets=all,`" line:

5ESS:

```
## Lucent Technologies 5ESS TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.60005,
cpnode=1;
```

DMS:

```
##  DMS SWITCH TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.9553,
dialstring2=TCP.<office_name>.9554,
dialstring3=TCP.<office_name>.9555,
authentication=Insecure,
max_maxcpt=20, max_tgxcpt=1024;
```

GTD5:

```
##  GTD5 SWITCH TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.10724,
max_maxcpt=65, max_tgxcpt=2000;
```

Some offices have only one dialstring that needs to be defined. By standard, that port number is 60005 for the *5ESS* and 10724 for the *GTD-5*. The *DMS* can have multiple dialstrings which can vary between *DMS* network elements.

The office name in all instances must be all lower case.

5ESS:

The cpnode number is also based on the office and assigned here. Unless there are multiple offices attached to the same ASM this should remain 1.

The <*office_name*> must match what is listed in the "/etc/hosts" file and what is used in the NTM system. It must also match what the ASM thinks the office is called.

---

5 In the "/musr/rb/tg" file add additional trunk groups to the trunk group file for any office utilizing enhanced trunk group monitoring.

This step is necessary only if you have purchased Surveillance of 1024 trunk groups.

---

6 In the "/musr/rb/rspte/rspte" file, add or modify a line for each office.

Ensure that the `direct=tcp` is at the end of the syntax as shown in these examples:

```
(5ESS) <office_name>,<hierarchy>,,<sets>,,
   ess5,5e15,1,y,tcp;
(DMS) <office_name>,<hierarchy>,,<sets>,,
   dms,na013,1,max_tg=1024 ,n,tcp;
(GTD5) <office_name>,<hierarchy>,,<sets>,,
   gtd5,gtd4003,1, ,n, tcp;
```

End Of Steps

□

Preparing the NTM host for migration to AI

Instructions

Prepare the NTM host for the conversion by:

- Collecting information required from the office
- Networking Setup (define switches in “/etc/hosts”, check “/etc/nsswitch.conf”)
- Record Base Changes

1 Make sure that both the network element and the NTM host recognize each others IP addresses. For the NTM hosts, this can be done through the “/etc/hosts” file.

2 Edit the “/nm/ubin/start.all” file.

In the file “/nm/ubin/start.all” the new data collectors must be defined: DCOL# where # is between 11 and 26. In total up to 16 new DCOLs can be defined. The numbering of the following DCOLs must be preserved for each type of DCOL.

Example for DCOL numbering:

```
DCOL11 - DCOL_5E
DCOL12 - DCOL_5E
DCOL15 - DCOL_DMS
DCOL16 - DCOL_DMS
DCOL17 - DCOL_DMS
```

3 In case the cutover needs to be backed out, save a copy of the original files for the:

- Office File
- RSPTE File

4 Update the office file for each office to be converted by replacing the “;” after `packets=all` with a “,” and inserting the following lines after the “`packets=all,`” line:

5ESS:

```
## Lucent Technologies 5ESS TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.60005;
```

DMS:

```
##  DMS SWITCH TECHNOLOGY
packets=all,
dialstring=TCP.<office_name>.9553,
dialstring2=TCP.<office_name>.9554,
dialstring3=TCP.<office_name>.9555,
max_maxcpt=20, max_tgxcpt=1024;
```

The office name in all instances must be all lower case.

The <*office_name*> must match what is listed in the "/etc/hosts" file and what is used in the NTM system.

The port numbers (e.g. "60005') are dependent on AI Switch configuration.

5 In the "/musr/rb/tg" file add additional trunk groups to the trunk group file for any office utilizing enhanced trunk group monitoring.

This step is necessary only if you have purchased Surveillance of 1024 trunk groups.

6 In the "/musr/rb/rspte/rspte" file, add or modify a line for each office.

Ensure that the `direct=ai` is at the end of the syntax as shown in these examples:

```
(5ESS) <office_name>,<hierarchy>,,<sets>,,
   ess5,5e15,1,y,ai;
(DMS) <office_name>,<hierarchy>,,<sets>,,
   dms,na013,1,max_tg=1024 ,n,ai;
```

END OF STEPS

□

Cutting over an office

Purpose

Switches do not support multiple, simultaneous interfaces for Network Management data. For this reason, the DCC interface cannot be maintained while the TCP/IP interface is in place. Removal of the entity definition from the DCC is necessary for this process. Otherwise, NTM will continue to associate the office with the DCC and not recognize the TCP/IP interface.

The following table outlines how to cut over an office from DCC to TCP/IP connectivity.

Instructions

Follow these steps to cut over an office:

1 Verify that the system time on the NTM host matches the system time on the office. The DCC/FEP will no longer be available to handle time differences. Execute the following command on each machine at the same time.

```
$ date
```

2 Verify the system time of the office is in synchronization with the NTM host.

Responsibility: This should be performed by the office administrator.

3 Switch the interface to TCP/IP

Responsibility: This should be performed by the office administrator.

4 DCC deprovision the entity.

Responsibility: This should be performed by the DCC administrator.

5 If the cutover will occur during the `dayend` process, comment out the “dayend” entry in the root crontab on the NTM host.

6 Verify that the system time on the NTM host matches the system time on the office. The DCC will no longer be available to handle time differences. Execute the following on each machine at the same time.

```
$ date
```

7 Deactivate the office by executing:

```
$ deact <office name>
```

8 Copy the modified RSPTE File and Office File into the appropriate directories; “/musr/rb/rspte/” and “/musr/rb/office/” respectively.

9 Test the RSPTE File by executing:

```
$ dbtest rspte
```

10 Examine the ouput to detect errors. If there are syntax errors, correct and repeat this step. If there are errors you are unable to correct, STOP and call Alcatel-Lucent support.

11 Update record base changes by entering:

```
$ create rspte
```

12 Enter:

```
$ stopsys
```

13 Enter:

```
$ installdb rspte now
```

14 Test the Office File by executing:

```
$ dbtest <office name>
```

15 Enter:

```
$ create office <office name>
```

16 Enter:

```
$ startsys
```

17 Check the link status of the converted office to verify that it is defined as TCP/IP direct connect and not associated with the DCC

```
$ linkstat <office name>
```

18 Verify the dcol assignment for the office.

```
$ /nm/dbutil/openstat m <office name>
```

Values should be:

- *5ESS* = DCOL 8
- *DMS* = DCOL 10
- *GTD5* = DCOL 12

19 Activate the converted office by entering:

```
$ act <office name>
```

20 Enter:

```
$ audit <office name> all
```

21 If you commented out the “dayend” entry in the root crontab on the NTM host in Step 5, uncomment the entry.

END OF STEPS

□

Backing out an office cutover

CAUTION

This activity should only be used if the conversion encounters a major problem and the decision is made to revert to the DCC interface. It is not part of the normal conversion procedure.

Some procedures cannot be reversed without significant hardware and/or software changes. This includes migrating 4ESS offices to TCP/IP connect via the DT4180.

Instructions

Follow these steps to change the office connection back to the DCC configuration.

1 Create and activate the entity on the DCC.

Responsibility: This should be performed by the DCC administrator.

2 Switch the interface to support the EADAS channel (TDM) or GPU (*GTD5*).

Responsibility: This should be performed by the Office Administrator.

3 Deactivate the office.

```
$ deact <office name>
```

4 Copy over the old RSPTE File, Office File, and Password File (*5ESS*) record base files.

5 Test the RSPTE File by executing:

```
$ dbtest rspte
```

Examine the ouput to detect errors. If there are syntax errors, correct and repeat this step. If there are errors you are unable to correct, STOP and call Alcatel-Lucent support.

6 Update record base changes by:

```
$ create rspte
```

7 Enter:

```
$ stopsys
```

8 Enter:

```
$ installdb rspte now
```

9 Test the office file by executing:

```
$ dbtest <office name>
```

10 Enter:

```
$ create office <office name>
```

11 Enter:

```
$ startsys
```

12 Check the link status of the converted office to verify that it is associated with a data collector.

```
$ linkstat <office name>
```

13 Activate the reverted office by entering:

```
$ act <office name>
```

14 Audit the reverted office by entering:

```
$ audit <office name> all
```

END OF STEPS

□

Verifying cutovers

Instructions

Follow these steps to verify cut overs:

1 Run linkstat to verify active state and data collection status.

```
$ linkstat <office name>
```

Verify that the Connection Status for each office on all three channels (HI, MED, LOW) all say “conn” (connected).

2 Run audits.

```
$ audit <office name> all
```

Verify that each audit runs to completion without any connectivity errors.

3 View data collection status by executing:

```
$ datastat <office name>
```

Verify that all configured packets (may not be all the listed packets) have FLAGS set to “GOOD”.

4 Execute sample controls (specific allowable controls must be determined by the customer for this test.) Verify that each properly defined control request is transmitted successfully to the office.

```
$ <ctrl> <office name> <parameters>
$ audit <office name> <equivalent control audit type>
```

Verify that the audit confirms the state your control should have established.

END OF STEPS

□

Finalize cutovers and deactivate the DCC interface

WARNING

This procedure should only be done when all offices have been removed from all DCC's and the DCC's are being decommissioned.

Instructions

Follow these steps to finalize cutovers and deactivate the DCC interface:

1 Remove or comment out DCC entries in the RSPTE File.

2 Remove or archive DCC Office Files.

3 Remove unused DCCs from the "/musr/ofclst/" directory.

4 Modify "/nm/ubin/start.all", turn off DCC DCOLs. (Set "respawn" to "off")

```
DCOL2:0:0:respawn:export SALI_MODE=urp;export
   SRVID=22;DCOL_FEP -s
DCAUDSVC2,DCADMSVC2,DCCTRLSVC2 -o /dev/null -e /dev/null -- -i
   2
```

Let the `dayend` process implement these changes.

END OF STEPS

□

Secure shell for Succession switches

Overview

Purpose

Procedures in this section provide information on configuration and installation of Secure shell for Succession switches.

Prerequisite Features

Secure connection for Succession switches is available only if all these features are purchased and installed:

- Feature 422, "Enhanced Security for Nortel Networks TR-746 Interface",
- Feature 432, "Enhanced Security for Nortel Networks Using sftp",
- Feature 433, "Support of Nortel Networks Succession SN08 Interface from SDM/CBM".

NTM is collecting data for Succession switches over a secure interface using the OPENSSH software package.

Generics

Succession (sn08+).

Contents

This section contains the following components:

□

Instructions

Verify the following on your system:

- SSH is installed.
- SSHD is running.
- HOST Key is created.
- Any other vendor based configuration.
- A default user is configured in the "/musr/rb/password" file. (This will be used to make the secure connections to the SDM. We recommend this default user to be defined as "vital".)
- The user vital has a home directory defined.
- For an existing office, the Secure Port numbers are the same as the port numbers in the Record Base Office File.
- Make sure the nmadm's public key is copied to vital's .ssh directory on the SDM (Step 3 in Installing Secure connection).
- Verify vital's home directory has permission of 755.
- Verify "~vital/.ssh" directory has permission of 700.
- Verify the "~vital/.ssh/authorized_keys2" has permission of 644.

Important! If authorized_keys2 file already exists, append the public key to the file.

□

Installing Secure connection

Instructions

Follow these steps to install Secure connection on NTM:

1 Login as nmadm.

2 Create the public key file /musr/nmadm/.ssh/id_rsa.pub for user nmadm by executing:

```
/usr/bin/ssh-keygen -t rsa
```

3 Copy the nmadm's public key to vital's authorized_keys2 file under the ".ssh" directory on SDM

Important! The public key should be created on all NTM systems that connect to a secure Succession office. The public key should also be copied to all the secure Succession elements that have the security enabled. Keys from multiple NTM systems (BDR) should be appended to the authorized_keys2 file. (Chapter 12, "BDR Administration on a Host")

4 If the NE is a new office, perform the following steps to create a new office:

- Add the NE information to the "/etc/hosts file",
- Add the login information to the "/musr/rb/password",
- Create the entry in the RSPTE File,
- Create the Office File in the office directory,
- In the Office File, make sure the authentication flag is set to Secure (`authentication=Secure;`)
- Create and Install the RSPTE and OFFICE files.

5 If the NE is an existing office, perform the following steps:

- In the office file, modify the authentication flag to Secure (`authentication=Secure;`)
- Create the office.

6 Start the NTM system by executing `startsys`.

7 Verify the data collection has resumed and is stable on all Successions.

□

Troubleshooting network elements issues

Overview

Purpose

This section contains information about common network connectivity issues.

Contents

This section contains the following components:

□

GSP connection problem

If error messages persist for any or all GSP switches, stating "can't communicate with DCOL X". Deactivate any recently modified switches or switch known to have network connectivity issues. This should resolve the error message. If the message persists, please contact Alcatel-Lucent customer support.

□

10 Time Synchronization

Overview

Purpose

This chapter provides information and procedures related to time synchronization.

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Specifying a synchronization switch" (p. 4)	5 minutes	X	
"Changing a synchronization switch" (p. 5)	5 minutes	X	
"Unspecifying a synchronization switch" (p. 6)	5 minutes	X	
"Configuring the time sync daemon on the host" (p. 10)	5 minutes	X	X
"Starting the time synchronization daemon" (p. 11)	5 minutes	X	X
"Stopping the time synchronization daemon" (p. 12)	5 minutes	X	X

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Checking the status of the time synchronization software" (p. 14)	5 minutes	X	X

Contents

This chapter contains the following topics:

□

Time synchronization — 4ESS

Overview

Purpose

This section describes time synchronization, which eliminates time differences between *4ESS* switches and NTM. You have the option of specifying a *4ESS* switch to use for synchronization or of using the NTM automatic selection algorithm.

NTM time is compared to the synchronization office every 5 minutes. If there is a difference greater than 4 seconds, a message records in the system error log. When there is a time difference greater than 4 seconds, the system time adjusts at the 4 minute 15 second mark of a period, and the adjustment message records in the error log. The time adjustment never exceeds 10 seconds within a 5-minute interval.

Contents

This section contains the following topics:

□

Specifying a synchronization switch

Instructions

Follow these steps to specify a synchronization switch:

1 To specify a synchronization switch, create a file named *"/nm/db/syncofc"* which contains the full office name (*Common Language* CLLI code) of an internal *4ESS* switch.

Result: After approximately 5 minutes, a status message will appear in the system error log, indicating that the specified switch will be used as the time synchronization office.

END OF STEPS

Errors

If the CLLI code is invalid or the *4ESS* switch is not internal, an error message from DCOL0 will appear in the system error log within 5 minutes. If this occurs, check the *"/nm/db/syncofc"* file to ensure that the CLLI code is valid and the *4ESS* switch is internal.

If the specified switch is not activated for discretes, then an error message will be logged every 5 minutes until the switch is activated or a different synchronization switch is chosen. Also, error messages will be logged every 5 minutes if an active switch is not responding to discrete polls.

□

Changing a synchronization switch

Instructions

Follow these steps to change a synchronization switch:

1 To change a synchronization switch, edit the *"/nm/db/syncofc"* file to contain a new office name.

Result: The system picks up the new name automatically.

END OF STEPS

□

Unspecifying a synchronization switch

Instructions

Follow these steps to unspecify a synchronization switch:

1 To unspecify a synchronization switch, remove the *"/nm/db/syncofc"* file.

Result: The system selects a new synchronization switch automatically and reports a status message in the system error log that indicates the new switch.

END OF STEPS

□

Inhibiting automatic time synchronization

Purpose

The file *"/nm/db/notimesync"* can be used to inhibit the automatic time synchronization. The file *"/nm/db/notimecheck"* can be used to inhibit reporting of time differences to the system error log. Use these files in the following manner:

- If *"/nm/db/notimesync"* exists and *"/nm/db/notimecheck"* does not, the NTM time will not be adjusted automatically. However, time differences between the synchronization switch and NTM will be reported in the system error log every 5 minutes.
- If *"/nm/db/notimesync"* exists and *"/nm/db/notimecheck"* exists, the time will not be adjusted automatically, and the time differences will not be reported to the system error log.

References

"linkstat" (p. 9) in the *Input Commands Guide*; also see the *System Responses Guide* for more information on the system error log.

□

Configuring time synchronization

Overview

Purpose

This section describes the procedure for configuring the HP's time synchronization on the NTM host.

> **Reference:** For additional information refer to *Configuring NTP (Network Time Protocol)* in the HP document *Installing and Administering Internet Services Guide.*

Contents

This section contains the following topics:

□

Configuring the time sync daemon on the host

Purpose

The configuration process can be performed on all NTM systems.

Important! If the *4ESS* Switch Time Synchronization feature is active, you must turn it off before starting the time synchronization daemon

Reference: "Stopping the time synchronization daemon" (p. 12)

Instructions

Follow these steps to configure the time synchronization daemon on the host:

1 Log into the system as `root`.

2 Use your favorite editor to edit the *"/etc/ntp.conf"* file.

3 Insert the following lines:

```
driftfile /etc/ntp.drift
server xxx.xxx.xxx.xxx
```

at the end of the file, where *xxx.xxx.xxx.xxx* is the network address of the UTC source.

Important! An example is provided in the file created during installation.

End Of Steps

□

Starting the time synchronization daemon

Purpose

After all configuration files have been properly modified, the time synchronization software must be started.

Reference: "Configuring the time sync daemon on the host" (p. 10)

Instructions

Follow these steps to start the time synchronization daemon:

1 Log into the system as `root`.

2 Use the system date command to set the system time to approximately UTC (the correct time where you are).

⚠ **WARNING**

The Time Synchronization Daemon will shut down within 20 minutes if the system time is more than 1000 seconds off UTC at startup.

3 Use your favorite editor to edit the *"/etc/rc.config.d/netdaemons"* file.

4 Modify the `export XNTPD = 0` entry by changing "`0`" to "`1`".

5 Save the file.

6 To start timesync, enter:

```
/etc/init.d/xntpd start
```

END OF STEPS

□

Stopping the time synchronization daemon

Instructions

Follow these steps to stop the time synchronization daemon:

1 Log into the system as `root`.

2 To stop timesync, enter:

```
/etc/init.d/xntpd stop
```

END OF STEPS

□

Configuring multiple time sources for HP’s time sync

Purpose

HP’s time sync can be configured to use multiple time sources for synchronization. This is accomplished by adding multiple server entries to the *“/etc/ntp.conf”* file (one entry per time sources). A preference can be set to use a particular source by adding the prefer keyword to the source’s server entry in the *“ntp.conf”* file. This will cause the preferred source to be used as the primary time sync source and all others to be used as secondary sources.

Figure

An example of the prefer keyword with multiple sources is given in Figure 1.

Figure 1 “ntp.conf” file entry — Prefer entry

```
server 155.55.5.5 prefer
server 155.55.6.6
```

□

Checking the status of the time synchronization software

Before you begin

Ensure syslogd is configured to log daemon information messages to the */var/adm/syslog/syslog.log* file. To check this configuration, make sure */etc/syslog.conf* includes on of the following lines:

```
*.info /var/adm/syslog/syslog.log
or daemon.info /var/adm/syslog/syslog.log
```

Instructions

Follow these steps to check the statue of the time synchronization software:

1. Log into the system as `root`.

2. Use the `ps` command to make sure the process “`xntpd`” is running on the system.

3. On the Host, check the *“/var/adm/syslog/syslog.log”* file for two start-up messages from xntpd.

   Result: The first message will show the software version and start-up time from xntpd. The second message will show kernel variables and their values.

   Important! These messages should appear immediately

4. After the software has stabilized and xntpd has done it’s first time modification, the file *“/var/adm/syslog/syslog.log”* on the host should contain a time reset entry from xntpd.

   Important! Stabilization may take from 5 minutes to several hours the first time the software is started on the machine.

END OF STEPS

□

11 Subnetwork Administration

Overview

Purpose

This chapter provides background and procedural information regarding administering subnetworks.

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Creating a subnetwork" (p. 6)	10 minutes	X	
"Deleting a subnetwork" (p. 9)	5 minutes	X	

Contents

This chapter contains the following topics:

□

Background

Overview

A ***subnetwork*** is a group of offices and trunk groups specified by the record base administrator in the NTM record base files. Subnetworks are used to automatically restrict a user's access to specified offices and trunk groups.

A user's access to network surveillance capabilities or the ability to put controls on the network is defined on a subnetwork basis. If Feature 3, “Management of Record Base Partitions and Subnetworks” is on, database modification permission can also be defined on a partition basis. Defining these capabilities on a subnetwork basis enables you to divide responsibility among users on one system.

Configuration

Subnetworks and user groups can be configured in a variety of ways to meet user needs. For example, you can set up user groups with full NTM functionality for a single subnetwork. You can also enable a user group to have surveillance capabilities for the whole network but to put controls on a smaller subnetwork.

The default maximum number of subnetworks is 2 in addition to the main subnetwork. Purchasable features increase the number of subnetworks you can have. If BDR is on the system, a maximum of 4 subnetworks may be defined (this includes the main subnetwork). Two of those four (including main) may be a partition. Otherwise, 3 subnetworks may be defined, main and 2 others. A partition is a subnetwork with a separate section of the record base. If Feature 3 is on, a maximum of 15 subnetworks may be defined. Up to 6 may be a partition (including main).

Characteristics of subnetworks

Subnetworks:

- use subnetwork permissions to determine which offices and/or trunk groups they can manage
- use permissions in *“/nm/etc/permissions”* to determine the commands that can be executed by members of a given user group
- are set up and maintained by an administrator in the snm group with the `snw_admin` command.
- allow users access to all system commands (as defined by their login permissions and application permissions)
- are backed up by BDR
- can be a partition

Subnetwork commands

Use the following two commands to create and administer the subnetworks:

- `snw_info` — Use this command to show the current list of subnetworks, user groups, and each group's subnetwork permissions. It can be run by anyone unless access is restricted by its entry in *“/nm/etc/permissions”*.
- `snw_admin` — Use this command to create and delete subnetworks and user groups and to set permissions. It is executable only by a member of the snm group.

□

Subnetwork permissions

Overview

Subnetwork permissions are defined for each user group on a subnetwork basis. There are two levels of permission:

- Full network management functions — The ability for surveillance, control, and auditing of offices and trunk groups in the subnetwork.
- Surveillance-only capability — The ability to see all network management data about the subnetwork, but not to execute controls or audits.

Permission types

It is possible for a user group to have surveillance, control, and audit permissions for one or more subnetworks and to have surveillance-only permissions for other subnetworks. A user in that group will be able to see network management information about any offices or trunk groups in subnetworks for which the user has surveillance, control, and audit, or surveillance-only permission. The user will be able to execute controls or audits only on offices and trunk groups for which the user has surveillance, control, and audit permission. For trunk group controls, it is possible to execute a control on a trunk group only if the user has surveillance, control, and audit permission on a subnetwork containing the trunk group and also on a subnetwork containing the from-office.

Database modification permissions

Customers with Feature 3, “Management of Record Base Partitions and Subnetworks” also may define database modification permissions for each subnetwork partition. Database modification permissions allow the user to run `create` and `dbtest` on offices in the partition. Database modification permissions can be assigned only for a partition, not for any other type of subnetwork.

□

Creating a subnetwork

Instructions

Follow these steps to create a subnetwork:

1 Log in as `nmadm` or some other user in the snm group.

2 Enter `snw_admin`.

Result: The main menu, shown in the Figure 1, appears. It lists the current subnetworks, valid user groups for each subnetwork, and a menu of administrative options.

3 Choose menu item `1` to create a new subnetwork. The system prompts you to enter a name for the subnetwork.

4 Enter the name of the subnetwork.

Hint: The subnetwork name can be 2 to 4 alphanumeric characters with the first character being alphabetical.

5 The system prompts you to specify whether the subnetwork is a partition. This prompt appears only if one of the BDR features (Feature 8, "Disaster Recovery (Duplex)" and Feature 40, "Enhanced Disaster Recovery") or Feature 3, "Management of Record Base Partitions and Subnetworks" is installed.

6 Enter `y` to make the subnetwork a partition or `n`.

Result: The system prompts you to enter `YES` to create the subnetwork.

7 Enter `y` to create the subnetwork.

Result: The system displays a message saying that the subnetwork has been created.

8 Enter 1 to return to the main menu.

9 To add user groups, complete the procedure in the "Adding and removing user groups" (p. 19).

10 Quit the `snw_admin` command by choosing the last item (quit) from the main menu.

11 Edit the record base RSPTE File to add the subnetwork to any offices that will be in the new subnetwork.

12 Edit the Trunk Group File(s) if desired to add the subnetwork to trunk groups.

Hint: By default, trunk groups will be in any subnetworks which contain either the to-office or the from-office. It is necessary to enter subnetwork information in the trunk group file only if you want to override the default subnetwork membership.

13 Do a `dbtest`, `create`, and `install` of the record base.

> **Reference:** "Performing a full create and installdb" (p. 3) in the *Record Base Administration Guide*

END OF STEPS

Figure

Figure 1 shows an example of the Subnetwork Administration Main Menu:

Figure 1 Subnetwork Administration — Main menu

```
09-07-93   13:15:41SUBNETWORK ADMINISTRATION
-----------------------------------------------------------------


   SUBNETWORK    TYPE                        USER GROUPS
  ------------  -----       ------------------------------------------------
      NMC          M            NM      RB      USR
      SUB1         P            SUB1NM
      SUB2         P            SUB2NM
```

```
-------------------------------------------------------------------------------

   MAIN MENU

  1. CREATE A NEW SUBNETWORK5. MODIFY NAME/PERMISSIONS
  2. DELETE AN EXISTING SUBNETWORK6. VIEW SUBNETWORKS
  3. ADD USER GROUP7. QUIT
  4. DELETE USER GROUP

   MENU OPTION:
```

□

Deleting a subnetwork

Instructions

Follow these steps to delete a subnetwork:

1 Remove all references to the subnetwork from the record base RSPTE File and Trunk Group File(s).

2 Do a `dbtest all`, `create all`, and `installdb all` of the record base.

Important! It is important that you execute all of these commands in order to make sure all the office and trunk group information is updated in the database.

Reference: "Performing a full create and installdb" (p. 3) in the *Record Base Administration Guide*

3 If you are deleting a subnetwork, you may need to remove the logins and user groups associated with the subnetwork.

Reference: "Removing user groups" (p. 23); "Removing users" (p. 5)

4 Enter `snw_admin`.

Result: The main menu, shown in Figure 1, appears.

5 Enter `2` (delete an existing subnetwork).

Result: The system prompts you to enter the name of the subnetwork to be deleted.

6 Enter the name of the subnetwork you want to delete.

Result: The system displays the message: `WARNING: You must also remove this subnetwork from the record base. Enter YES to delete the subnetwork.`

7 Enter `y` to delete the subnetwork.

Result: The system displays a message telling you that the subnetwork has been deleted.

Any user group permissions for this subnetwork are removed at this time. If any user groups had this subnetwork for their home subnetwork, they are moved to the main subnetwork.

8 Enter `1` to return to the main menu.

Result: The main menu is displayed.

9 Enter `7` to quit the main menu.

END OF STEPS

□

12 BDR Administration on a Host

Overview

Purpose

BDR (Backup and Disaster Recovery) is optional. It is available only if Feature 8, “Disaster Recovery (Duplex)” and Feature 40, “Enhanced Disaster Recovery” has been purchased.

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
“Configuring hosts for BDR” (p. 15)	1 hour	X	
“Performing system administration tasks” (p. 24)	15 minutes	X	
“Performing record base administration tasks” (p. 25)	1 hour	X	
“Performing system administration tasks” (p. 24)	45 minutes	X	
“Checking the state of BDR on a host” (p. 28)	5 minutes	X	

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Activating BDR on a host" (p. 29)	5 minutes	X	
"Deactivating BDR on a host" (p. 30)	5 minutes	X	
"Checking global record base file status — host" (p. 32)	5 minutes	X	
"Changing global record base file state — primary" (p. 33)	5 minutes	X	
"Changing global record base file state — backup" (p. 34)	5 minutes	X	
"Changing global record base file state — inactive" (p. 35)	5 minutes	X	
"Taking over operations — Failed host" (p. 38)	30 minutes with minimal audits; 2 to 3 hours if the "`audit =all`" option is selected.	X	
"Taking over operations — DCC" (p. 42)	15 minutes without audit; up to 2 hours with audit	X	
"Taking over operations — TCP/IP connected switch" (p. 44)	5 minutes	X	
"Taking over operations — Non-failed host" (p. 46)	45 minutes without audits; 3 to 4 hours with audits	X	
"Synchronizing record base files with another host" (p. 49)	5 minutes	X	
"Returning operations to the original host" (p. 50)	30 minutes without audits; 2 to 3 hours with audits	X	
"Returning operations to original host — DCC or TCP/IP" (p. 53)	15 minutes without audit; up to 2 hours with audit	X	
"Returning operations to original host — Single DCC" (p. 54)	15 minutes without audit; up to 2 hours with audit	X	
"Returning operations to original host — TCP/IP" (p. 55)	5 minutes	X	
"Backing up the DCC_Alias file" (p. 58)	5 minutes	X	

Contents

This chapter contains the following topics:

□

Quick reference

Purpose

These quick references tables are intended as clear and concise procedures for users who are not necessarily familiar with BDR commands, but who may find themselves needing to perform BDR takeover and switchback in an emergency situation.

Before you begin

Before starting, check DCCs to determine if the hostnames are current.

Tables

Table 1 provides a quick reference chart for takeover functions. Table 2 provides a quick reference chart for switchback and restore functions.

Table 1 Quick reference — Takeover

Step	As user ...	Enter ...	Comments
On host that will give up its offices:			
1	nmadm	`$ linkstat`	
2	nmadm	`$ ps -ef | grep installdb`	Verify that “installdb” is not running.
3	nmadm	`$ ps -ef | grep audit`	Verify that “audit all all” is not running.
4	nmadm	`$ deact` *<4ess cllis>*	
5	nmadm	`$ linkstat typ=ess4`	
6	nmadm	`$ stopsys`	
On host where takeover will be:			
7	nmadm	`$ act` *<4ess cllis>*	
8	nmadm	`$ bdr_takeover` *<hostname>*	Where <*hostname*> is the host to give up its offices. Exception printer responds with a “n”
9	nmadm	`$ linkstat`	verify status of DCC and 4ess links

Table 2 Quick reference — Switchback and restore to individual hosts

Step	As user …	Enter …	Comments
On host where all offices are:			
1	`nmadm`	`$ bdr_switchbk <hostname>`	Where <*hostname*> is the Linux host to be restored with its offices.
2	`nmadm`	`$ linkstat`	
On host for offices to be restored to itself:			
3	`nmadm`	`$ startsys`	
4	`nmadm`	`$ act 4ess <clli>`	
5	`nmadm`	`$ linkstat`	
6	`nmadm`	`$ audit all all`	
Verify status of switchback on both hosts			
7	`nmadm`	`$ sysstat`	
8	`nmadm`	`$ linkstat`	After running `linkstat` command, monitor the errors file

□

BDR feature description

Purpose

BDR allows two or more NTM host computers, each of them supporting one or more Network Traffic Management (NTM) center, to provide backup and disaster recovery for each other, as well as for each other's NTM centers. In other words, BDR allows an NTM host to take over the operations of another host and for an NTM center to take over the operations of another NTM center.

Capacity

Each host must have sufficient capacity to manage its individual offices as well as the offices of those hosts for which it is designated as backup host. The connections between hosts must be over high-speed Ethernet TCP/IP lines. Figure 1 shows a simplified example of an NTM architecture that would support BDR.

With only two hosts in the BDR configuration, Host A and Host B, Host A will back up Host B and Host B will back up Host A. With more than two hosts in the BDR configuration, multiple back up scenarios are possible. For instance, in a three host BDR configuration, if one host cannot be sized to handle the traffic for the entire network (cannot serve as backup for both of the other hosts), a "daisy chain" configuration may be implemented. This configuration allows each host to be the back up for one other host. For example, with host names Host A, Host B, and Host C, Host B backs up Host A, Host C backs up Host B, and Host A backs up Host C.

Treatment of error messages

The BDR-specific status and error messages are logged in the *"/musr/log/bdrlog"* file. This file, as well as the standard message file (*"/musr/log/errors"*) should be monitored on a regular basis and any problems reported should be corrected as quickly as possible, to ensure that the machines remain synchronized with each other.

Reference: See the *System Responses Guide* for additional information on specific messages in either file.

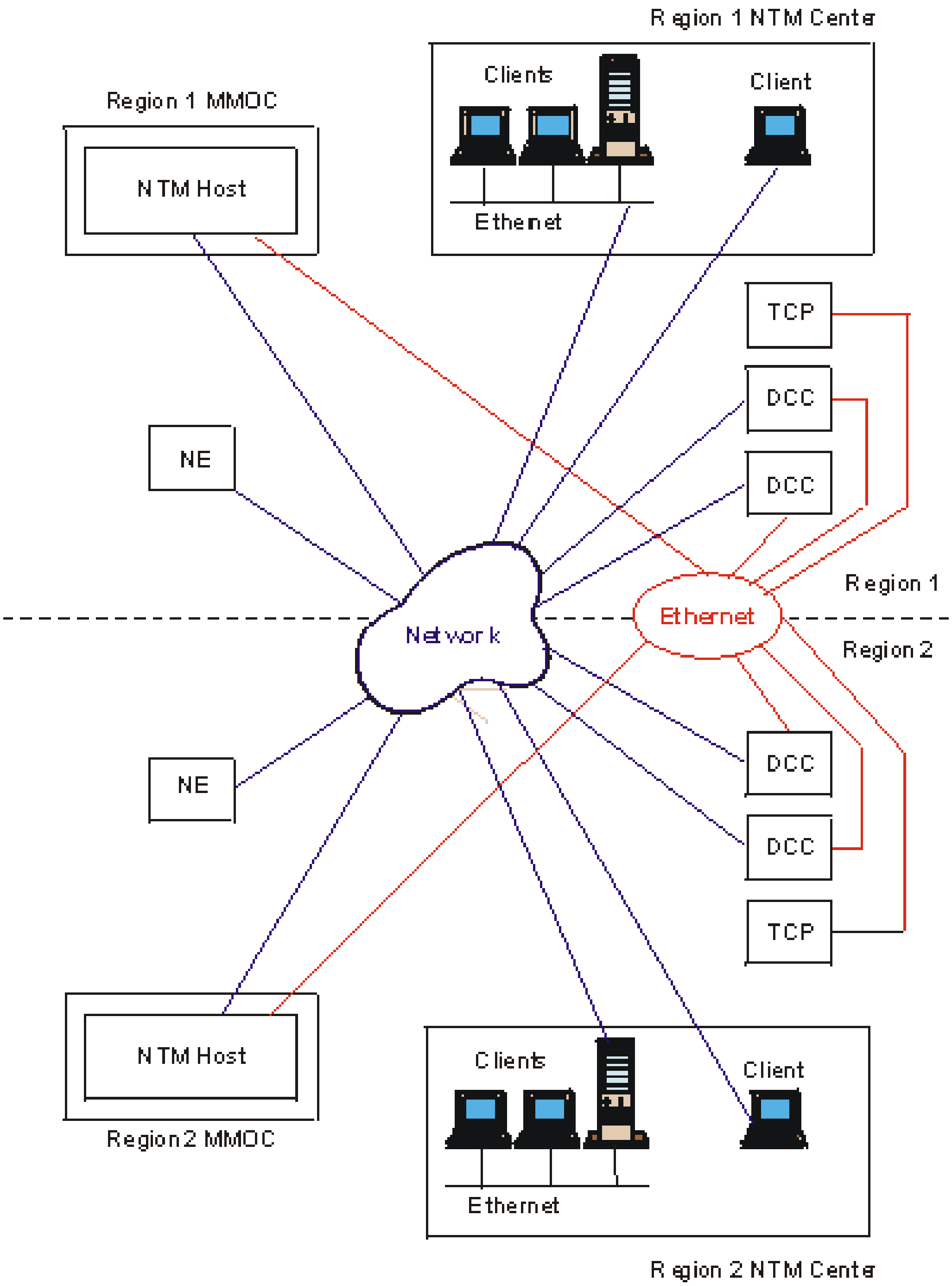
Using SSH with BDR

It is recommended that users perform BDR functions using Secure Shell (SSH) when transferring information between hosts during the BDR process. Beginning with NTM release 15, an SSH feature is available within NTM. Contact Alcatel-Lucent customer support to enable this feature. The SSH server must be installed and operating before initiating a BDR procedure. For more information on SSH, see "Secure shell for BDR" (p. 27) in the *Installation Guide*.

UDDM/UDNEI offices

The BDR feature fully supports replication of the UDDM/UDNEI offices. This applies to network elements that are defined as UDNEI elements or to elements that are defined as “traditional” element, but with a udneitype associated with them. Hovewer the files *“/musr/rb/udnei/udneitype”* and *“/musr/rb/udnei/<dcol>/dcol_params”* must be manually syncronized (See Synchronizing UDDM/UDNEI files for BDR in the *Record Base Administration Guide*).

Figure 1 NTM architecture for BDR



□

Scenarios

Overview

BDR supports a backup capability for the following failure scenarios:

- An NTM center “fails”, that is, becomes unusable, and the center's operations are transferred to another NTM center.
- An NTM host “fails” and the operations of the NTM center supported by that host are supported by another NTM host.
- An NTM host and one or more NTM centers it supports “fail.” The operations of the failed centers are transferred to working centers that are supported by another NTM host.

Each of these three scenarios is described in more detail in the next sections.

Scenario #1 — Single NTM center fails

A single NTM center “fails”, that is, becomes unusable, and the center's operations are transferred to another NTM center.

If a NTM center fails (becomes unusable), another working NTM center, supported by the same or a different NTM host, may take over the responsibility for monitoring and controlling the offices supported by the failed NTM center. Using local clients in their own center, personnel in the working NTM center may log in to their own host or to the backup NTM host and request all the necessary data required to monitor and control the offices supported by the failed NTM center.

Scenario #2 — NTM host fails

An NTM host “fails” and the operations of the NTM centers supported by that host are supported by another NTM host.

If the system administrator on the working NTM host decides that it is necessary to provide backup support for the failed NTM host and he or she performs a takeover procedure that activates the offices in the other region. This causes the working NTM host to establish data connections to the corresponding offices (for example, *4ESS* switches) and to the appropriate data collection concentrator (DCC) systems, for example, the Engineering and Administrative Data Acquisition System (EADAS).

It is assumed that raw traffic data is up to date only on the primary NTM host (the NTM host supporting normal operations for a center and not providing backup operations support). When a failure of the primary NTM host occurs and the takeover procedure has been successfully performed on the backup NTM host, the backup NTM host begins to collect raw data from the supported regions of both NTM systems; but it has historical data only for its primary offices. As time goes on, the backup NTM host will accumulate data for both regions.

Scenario #3 — Host and center fail

An NTM host and one or more of the NTM centers it supports "fail." The operations of the failed centers are transferred to working NTM centers that are supported by another NTM host.

This failure scenario is the sum of failure Scenarios 1 and 2. Thus, the takeover for this failure scenario is the same as for Scenarios 1 and 2, except that personnel in the working NTM centers will take over responsibility for monitoring and controlling offices in the failed region using their terminals and host. Note that personnel in the backup NTM center do not log in to the NTM host of the failed NTM centers because the NTM host supporting such a center also has failed.

Scenario #4 BDR Takeover appears to not recognize network elements

BDR_takeover and BDR_switchback scenario in which offices may not be activated or deactivated.

Normally, the bdr-takeover command activates and the bdr_switchbk command deactivates the DCCs and offices on the NTM backup host. There can be a scenario where the NTM host has been reloaded, the DCCs have been renamed, or a new host machine is added. Since the DCCs have never been activated on the NTM backup host, it does not have a list of offices names to associate with that specific DCC. Without the list of office names, the BDR process does not know which offices need to be activated or deactivated.

Because of the flexibility of BDR to takeover and switchback; offices, DCCs, or an NMS, BDR takeover and switchback commands cannot just blindly activate/deactivate all of the offices and DCCs. Therefore, if a machine has recently been reloaded, changed a name of a DCC, or added a new NTM host, you will need to run the act/deact commands for the DCCs and offices on the NTM backup host after the bdr_takeover or bdr_switchbk commands have completed.

□

BDR audit and control synchronization

Overview

During normal operation, all audit and control results on the primary host are backed up in real time to all backup hosts, provided that the link between the hosts is operational and backup hosts are up and running. This allows users to have current audit and control information immediately after BDR takeover of another host is performed.

Any control information written into the control log is transmitted to and stored in real time in the control log of the backup hosts. The system also keeps track of all controls taken out after the last audit performed for each office. These procedures are transparent and do not require any user interactions.

Audit results

When a successful audit is executed, the audit result is transmitted in real time to all backup hosts and is stored in their databases as well as in the database of the primary host. The audit results also are stored in *Linux* system files (on the primary host) whenever they are written into the database.

The real time synchronization of audits and controls cannot be performed if there is a communication link outage or if the backup host is down. The end of day procedures of the BDR will synchronize any audits or controls that were not synchronized in real time as long as the communication links and/or the backup host are restored.

Marked alarms

Another aspect that is maintained through BDR is the synchronization of marked alarms when Feature 379, “Marked Alarm Persistence on BDR” is purchased.

□

End-of-day operations with BDR

Overview

During the end-of-day operations, all offices that had controls taken out after they were last audited will be audited. As mentioned earlier, the system keeps track of all controls taken out after the last audit performed for each office. These audits will ensure that all controls are synchronized between primary and backup hosts.

To ensure that all audits are synchronized during end-of-day procedures, the system compares the audit result files on the backup host with those on the primary host. Audit result files on the backup host that are different will be synchronized with the audit result files on the primary host. Once all audit result files are synchronized, the information in all files copied from the primary host is inserted into the database (this procedure is described in the recreate procedure for BDR).

local_audit

The audit result files also are used by the `local_audit` command to repopulate the database with the audit and control information for backup offices after the database is reconfigured (for example, after `create all`).

Monitor the *"/musr/log/bdrlog"* and *"/musr/log/errors"* files to detect any problems with the real time audit and control synchronization. These problems usually are caused by communication link failures or the unavailability of the backup hosts.

End-of-day procedures performed by the recreate command

With BDR, the following procedures will be performed by the `recreate` command as part of the end-of-day procedures,

Monitor the *"/musr/log/recreate.out"*, *"/musr/log/bdrlog"*, and *"/musr/log/errors"* files to detect problems with end-of-day procedures. Also monitor the "recreate.out" file to make sure that no errors were found during the create, activate, or audit procedures.

Table

Table 1 provides an overview of the different end-of-day procedures performed by the `recreate` command.

Table 3 Procedures Performed by the recreate command (Sheet 1 of 2)

Item #	Procedure
1	The other hosts are checked for any global record base files in PRIMARY state. If any global files are found to be in the PRIMARY state on the other hosts, they are copied to this host (the host on which `recreate` is executed).
2	The backup record base partitions on this host are synchronized with the hosts that are primary for those partitions. Any record base files that are different are copied from the primary host.
3	All record base partitions are searched for record base files that have been modified since the last `installdb` or `recreate`.
4	For all modified (if any) record base files that are not office related: • `dbtest` is executed for the file(s) • If `dbtest` does not find errors, `create` is executed for the file(s). • If `create` does not find errors, `installdb` is executed for the file(s). If the NTM application must be stopped before the file(s) can be installed, `stopsys` and `startsys` are executed before and after `installdb` respectively. The `installdb` for all files (if any) is done in one step so only one `stopsys`/`startsys` is necessary.
5	For all modified (if any) record base files that are office related and are in the primary partitions: • `dbtest` *single-office* is executed for the file(s) • If `dbtest` finds errors, nothing else will be done for the office. You must fix the errors manually before you proceed. • If the office is active, it is deactivated. • `create` *single-office* is executed for the file(s) • If the office was active originally, then it is activated for audit only. • If the office was activated, an audit is performed. The audit type depends on the type of office. The office's activation mode is returned to its original state.
6	Audits then are performed remotely on the primary hosts for offices that meet the following criteria: • This host is the backup host for the office. • At least one control has been taken out on the primary host for this office since it was last audited. This is to ensure that the audit information is up to date on the backup host.
7	All audit response files for backup offices are synchronized with files on the primary hosts for those offices. Audit response files that are different on the backup host are copied over from the primary host.

Table 3 Procedures Performed by the recreate command (Sheet 2 of 2)

Item #	Procedure
8	For all modified (if any) record base files that are office related and are in the backup partitions: • `dbtest` is executed for this file • If `dbtest` finds errors, nothing else is done for the office. You must fix the errors manually before you proceed. • `create` *single-office* is executed for this file Audit information in the database is updated from the audit response files (if any exist).
9	Audit information in the database is updated for all audit response files that were copied over from primary hosts during the synchronization procedure (if any).
10	If `recreate` detects that new offices have been added or some offices were not configured properly before, it will execute `stopsys`/`startsys` again to update the information about these offices. Since the time of this `stopsys`/`startsys` is unpredictable and depends on the amount of work `recreate` must perform, a wall message is sent out to notify everyone on the system that the NTM application will be stopped. A short period is provided for users to kill the `recreate` process before it stops the NTM application if they are performing a critical operation and do not wish the system to stop.

□

Configuring hosts for BDR

Purpose

The following is a description of the procedures that must be performed to configure BDR on an NTM host. You also can use it as a checklist during configuration and maintenance of BDR.

Commands

Most BDR and record base-related commands must be able to copy files to and execute commands on the other hosts. Users who execute these commands must have appropriate permissions on all hosts. Therefore, these users must have logins on all hosts.

Files

All record base files also must have appropriate *Linux* system permissions for the affected users.

Features

When Feature 22, “NMADM Login Accountability”, and Feature 8, “Disaster Recovery (Duplex)” and Feature 40, “Enhanced Disaster Recovery” are installed, certain commands are logged in the cmdlog file on both the primary and backup hosts. If a non-standard security system is installed, the command log may not report the same user ID on the backup host as it does on the primary host.

Instructions

Follow these steps to configure hosts for BDR:

1 Make sure that BDR is available on all hosts. This is usually performed automatically as part of the software installation procedures. (The term “host” here refers to an NTM host that is involved in BDR).

2 Define the names of all hosts and their internet numbers in the *“/etc/hosts”* file. Refer to the *Linux* system guides for information about the *“hosts”*(5) file.

> **Important!** Note that dash signs (-) are not allowed in the host names.

3 Enter the nms entity name in the *“/musr/rb/rspte/rspte”* file on each host.

Reference: "RSPTE File" (p. 68) in the *Record Base Administration Guide*

4 Add a login ID to the *"/etc/passwd"* file for each of the other NTM hosts. The login ID should be the name of the other host(s) as displayed in the *"/etc/hosts"* file. The entry must be in the format *uname*.domain.

The following is an example of a command to be executed to add a login ID for NTM host "hostB" on NTM host "hostA":

```
useradd -g 902 -c "Dummy login for NTM BDR feature" -M -s
   /sbin/nologin hostB
```

The following is an example of a passwd entry in the *"password"* file for NTM host *"hostB"* on NTM host *"hostA"*:

```
hostB:x:1003:902:Dummy login for NTM BDR
   feature:/home/hostB:/sbin/nologin
```

In some instances a *"shadow"* file will exist. The following is an example of a "shadow" entry in the *"/etc/shadow"* file for NTM host *"hostB"* on NTM host *"hostA"*.

```
hostB:!!:14673:0:99999:7::::
```

These login entries are used by NTM commands to display the name of another host, when appropriate. For example, for controls taken by host "hostB", the `ctrlog` command on "hostA" will display the name "hostB" as the name of the user taking the control. This will show that the control was taken by someone in host "hostB".

These login entries do not need a password or a home directory.

5 Configure record base partitions for each host using the `snw_admin` command. The name of record base partitions must be the same on all hosts and must be unique within each host.

Reference: Chapter 11, "Subnetwork Administration"; "snw_admin" (p. 17) in the *Input Commands Guide*

6 Configure groups for each host using the `snw_admin` command. All group names do not have to be the same on all systems, but appropriate user groups and permissions should be defined so that it is possible for users to log in to any host necessary.

Reference: Chapter 3, "System Security, User Groups, and Group Permissions"; "snw_admin" (p. 17) in the *Input Commands Guide*

7 Add users to the groups. If users already exist but the groups they should use have changed, modify the group and passwd files to indicate the new group. Users must have the same login ID on all hosts they need to access.

Reference: Chapter 2, "Adding and Removing Users on the Host"

8 Decide which collectible network entities are managed by each host. Then define these entities in the rspte and other record base files.

Reference: Chapter 9, "Maintaining the Record Base with BDR" in the *Record Base Administration Guide*

Important! For the "daisy chain" configuration described in the "BDR feature description" (p. 6), internal entities in one host may have to be defined as external entities on another host. For example, where hostB is backing up hostA, host C is backing up hostB, and hostA is backing up host C, internal entities on hostA may have to be defined as external entities on hostC.

9 Create the *"/musr/rb/part_perm"* file (using "Configuring the "/musr/rb/part_perm" file" (p. 22)) to define the desired permissions of the record base files for each record base partition.

Hint: When copying files from one host to another, BDR will set the permission of each copied file according to the partition it is moved to and the permissions defined in the "/musr/rb/part_perm" file for that partition.

10 Build an empty office record base file for each nms entity (in *"/musr/rb/office"* directory).

Reference: Chapter 9, "Maintaining the Record Base with BDR" in the *Record Base Administration Guide*

11 Build the inms record base file (in *"/musr/rb/inms"* directory) to define primary and backup hosts for each record base partition. Only record base partitions used in conjunction with BDR need to be defined in the inms file.

Reference: "INMS File" (p. 31) and Chapter 9, "Maintaining the Record Base with BDR" in the *Record Base Administration Guide*

Each host should be assigned as primary for record base partitions managed by that host. However, only one host should be assigned as primary for each partition.

For each record base partition, another host must be assigned as the backup host.

12 Execute `dbtest all`, `create all`, and `installdb all`, as appropriate.

> **Important!** We strongly recommend that you use the `dbtest all`, `create all`, and `installdb all` commands. If you do not want to use these commands (due to time constraints or other factors), you may use the following procedure:
>
> 1. Execute `dbtest rspte`, `create rspte`, `dbtest inms`, and `create inms` after the rspte and inms record base files have been configured properly.
> 2. If the NTM application is running, stop it by executing `stopsys`.
> 3. Execute `installdb rspte` and `installdb inms`.
> 4. After the procedures have been performed successfully, start the application again by executing `startsys`.

13 Follow this decision tree:

- If this is a new system that has never been booted, go to the next step.
- If this is a system that has never been booted without BDR, execute the following commands to start the DCOL1 and NMSRCV processes:

```
/nm/ubin/admsys DCOL1 respawn
/nm/ubin/admsys NMSRCV respawn
```

14 Execute `/nm/sys/bdr_act` to activate BDR.

> **Important!** Before executing `bdr_act`, the application must be running or have been started (using `startsys`) at least once since the NMS entities were added to the system. If `startsys` has never been run, `bdr_act` will not work.
>
> **Reference:** "Activating BDR on a host" (p. 29); "bdr_act" (p. 5) in the *Input Commands Guide*

15 As a part of normal operations, monitor the *"/musr/log/bdrlog"* file for status of BDR and correct any problems that are reported as soon as possible.

Also, monitor the outcome of dayend procedures (reported in mail to the system administrator), the "/musr/log/recreate.out" file, and the status of the links (with the `linkstat` command).

16 Before modifying global record base files (the `bdr_chgstat -s all` command lists all defined global record base files), change their state to PRIMARY first, using the `bdr_chgstat` command.

Be sure to change the state of these files to BACKUP after you have made changes and have successfully executed the appropriate `create` commands to allow other users on other hosts to make changes to these files.

These files are synchronized only when they are in the PRIMARY state and the appropriate `create` or `dbtest` commands are executed.

Global files are intended to stay in the BACKUP state until a change is required.

Reference: "bdr_chgstat" (p. 7); "create" (p. 5); "dbtest" (p. 17) in the *Input Commands Guide*

17 Periodically (monthly, for example), run the `create all` and `installdb all` commands to make sure that the record base and the databases are configured properly.

END OF STEPS

□

Configuring record base partitions

Overview

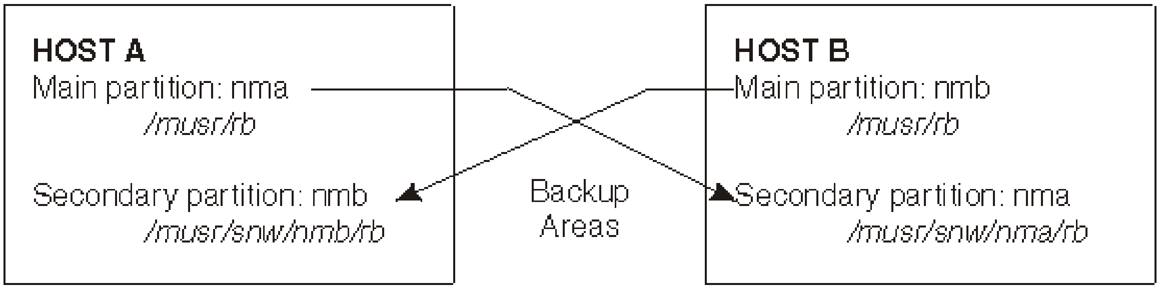
In order to back up record base files between hosts, you must configure the record base partitions correctly. There must be a record base partition on each host that contains the offices that are primary on other hosts. This partition must have the same name as the main record base partition on the other hosts.

For example, if Host A has a main record base partition with the name "snwa" and Host B has a main record base partition with the name "snwb", then a record base partition must be created on Host B with the name "snwa".

Figure

Figure 2 illustrates the setup of two hosts and their partitions, and how the two interact for backup purposes.

Figure 2 Primary and secondary host partitioning



Two-host BDR

Two record base partitions (including main) can be defined on each host for a two-host BDR. For a BDR configuration with more than two hosts, additional record base partitions are needed. These additional partitions are made available through Feature 3, "Management of Record Base Partitions and Subnetworks", which allows a total of six record base partitions (including main). With BDR, it is necessary for all hosts to have the same record base partitions so that record base files related to offices and trunk groups in those record base partitions can be created correctly on all systems. User groups do not have to be the same on all systems, but appropriate user groups and permissions should be defined so that it is possible for users in a center to log in to any host as necessary in an emergency.

References

Chapter 2, “Managing Record Base Partitions” in the *Record Base Administration Guide*

□

Configuring the “/musr/rb/part_perm” file

Overview

The *“/musr/rb/part_perm”* file contains permission information for record base files in each record base partition. This file should be created to define the desired permissions of the record base files for each record base partition. When copying files from one host to another, BDR sets the permission of each file it copies according to the partition it is moved to and the permissions defined in the *“/musr/rb/part_perm”* file for that partition.

Required information

For each record base partition, a single line with the following information is required:

- record base partition name
- mode
- owner
- group

Items are separated by any number of blank spaces and/or tab characters.

The *“record base partition name”* must be at the beginning of a line. All lines without a *“record base partition name”* at the beginning of the line are ignored. The *“record base partition name”* must be the name of the record base partition or *“main”* for the main partition.

The *“mode”*, *“owner”*, and *“group”* entries are standard *Linux* system permissions.

Figure

Figure 3 shows an example of entries in the *“/musr/rb/part_perm”* file.

Figure 3 “/musr/rb/part_perm” file

```
main 777 nmadm snm
south 775 rbsouth nm
north 444 rbnorth nm
```

□

Configuring record base files for BDR

Overview

Purpose

The following procedures provide the steps to be taken to configure the record base files for BDR.

The record base administration tasks are explained in detail, with examples, in “Configuring the record base files for BDR” (p. 7) in the *Record Base Administration Guide*.

Contents

This section contains the following topics:

□

Instructions

Follow these steps to perform system administration tasks:

1 Create the appropriate partitioned subnetworks.

Reference: Chapter 11, “Subnetwork Administration”; “snw_admin” (p. 17) in the *Input Commands Guide*

END OF STEPS

□

Performing record base administration tasks

Before you begin

Throughout this procedure, note that the main partitioned subnetwork record base files reside under the *"/musr/rb"* directory structure. The remaining partitioned subnetwork record base files reside under the *"/musr/snw/<partition>/rb"* directories.

Instructions

Follow these steps to perform record base administration tasks:

1 Move or copy the RB files for all partitions to the proper partitioned RB directory.

2 Add all hosts to the *"musr/rb/rspte/rspte"* file.

Hint: One entry for each host needs to exist in the appropriate RSPTE File.

Reference: "RSPTE File" (p. 68) in the *Record Base Administration Guide*

3 Create an empty office file for each host in the "/musr/rb/office" directory.

Reference: "Office File" (p. 40) in the *Record Base Administration Guide*

4 Create and install the rspte file.

5 Modify the *"/musr/rb/inms/inms"* file to reflect any new partitions.

Reference: "INMS File" (p. 31) in the *Record Base Administration Guide*

6 Create and install the *"/musr/rb/inms/inms"* file.

END OF STEPS

□

BDR on a host

Overview

Purpose

The following procedures relate to BDR on a host.

Contents

This section contains the following topics:

□

Checking the state of BDR on a host

Purpose

Both the `/nm/sys/bdr_act` and `/nm/sys/bdr_deact` commands first display the current status of BDR and then prompt you to specify if you wish to continue. If you only want to check the current status, enter `n` at the "`Continue? [y/n]`" prompt.

Instructions

Follow these steps to check the state of BDR on a host:

1 Log in to the host as `nmadm`

2 Enter `/nm/sys/bdr_act`

Result: The status of BDR is displayed as active, not active, or undefined.

Important! Before executing `bdr_act`, the application must be running or have been started (using `startsys`) at least once since the NMS entities were added to the system. If `startsys` has never been run, `bdr_act` will not work.

3 Enter `n` at the prompt "`Continue? [y/n]`"

END OF STEPS

□

Activating BDR on a host

Instructions

Follow these steps to activate BDR on a host:

1 Log in to the host as `nmadm`

2 Enter `/nm/sys/bdr_act`

Result: This command changes the state for the entire BDR to ***active*** on an NTM host.

BDR in the ***active*** state enables the application software on this host that performs backups to other hosts and allows other hosts to back up data on this host.

Important! Before executing `bdr_act`, the application must be running or have been started (using `startsys`) at least once since the NMS entities were added to the system. If `startsys` has never been run, `bdr_act` will not work.

Reference: "bdr_act" (p. 5) in the *Input Commands Guide*

3 Press `y` at the prompt "`Continue? [y/n]`"

END OF STEPS

□

Deactivating BDR on a host

Instructions

Follow these steps to deactivate BDR on a host:

1 Log in to the host as `nmadm`

2 Enter `/nm/sys/bdr_deact`

Result: This command changes the state for the entire BDR to ***INACTIVE*** on an NTM host.

BDR in ***INACTIVE*** state disables the application software on this host that perform backups to other hosts and inhibits other hosts from backing up data on this host.

3 Press `y` at the prompt "`Continue? [y/n]`"

END OF STEPS

□

Global record base administration for BDR

Overview

Purpose

Use the following procedures to check the status of all global record base files on a host, and to change the status of a global record base file to PRIMARY, BACKUP, or INACTIVE.

Contents

This section contains the following topics:

□

Checking global record base file status — host

Instructions

Follow these steps to check the status of a global record base file on a host:

1. Log in to the host as `nmadm`

2. Type `bdr_chgstat -s all`

   Result: The status of all global record base files for that host is displayed.

   Reference: “bdr_chgstat” (p. 7) in the *Input Commands Guide*

END OF STEPS

□

Changing global record base file state — primary

Purpose

In the PRIMARY state, the global record base file will be backed up to all other hosts on which this file is in the BACKUP state. The contents of the file on other hosts will be overwritten with the one from this host. This backup is performed as part of the end-of-day procedures or when `dbtest` or `create` commands are executed for the global file. Users on other hosts are not permitted to overwrite the contents of the global file on this host as long as it is in the PRIMARY state. However, the PRIMARY state is intended to be used for changes only. Once changes have been completed and the appropriate `create` commands have been executed, the file should be returned to the BACKUP state.

Instructions

Follow these steps to change the state of the global record base file to primary:

1 Log in to the host as `nmadm`

2 Type `bdr_chgstat -p` *`global_file_pathname`*

Result: The state of the global file is changed to PRIMARY if the file is not already in the PRIMARY state on another host.

Reference: "bdr_chgstat" (p. 7) in the *Input Commands Guide*

END OF STEPS

□

Changing global record base file state — backup

Purpose

In the BACKUP state, the file is not backed up to other hosts. Another host that has the PRIMARY state for the same global file is permitted to back up any changes for the global file to this host.

Instructions

Follow these steps to change the state of the global record base file to backup:

1 Log in to the host as `nmadm`

2 Type `bdr_chgstat -b` *`global_file_pathname`*

Result: The state of the global file is changed to BACKUP.

Reference: "bdr_chgstat" (p. 7) in the *Input Commands Guide*

END OF STEPS

□

Changing global record base file state — inactive

Purpose

In the INACTIVE state, the file is not backed up to other hosts nor are other hosts permitted to back up their changes for the global file to this host.

Instructions

Follow these steps to change the state of the global record base file to backup:

1 Log in to the host as `nmadm`

2 Type `bdr_chgstat -i` *`global_file_pathname`*

Result: The state of the global file is changed to INACTIVE.

Reference: "bdr_chgstat" (p. 7) in the *Input Commands Guide*

END OF STEPS

□

BDR take-over/switch-back system administration tasks

Overview

Purpose

The following procedures are provided for taking over operations responsibility for a host, Data Collection Concentrator (DCC), or switch and for switching operations responsibility back to a host, Data Collection Concentrator (DCC), or switch.

Before you begin

Before a disaster occurs and as part of normal operations, make sure that the record base, and database, are configured correctly on all hosts.

Because these procedures must be done during a disaster situation, we recommend that the audits portion be executed only when necessary; this should reduce any performance degradation.

Contents

This section contains the following topics:

□

Taking over operations — Failed host

Purpose

The following procedure should be performed when a host (referred to here as Host B) must take over the functionality of another host (referred to here as Host A) that has failed. When this procedure is completed, Host B takes over the data collection and network management operations for Host A.

Before you begin

This procedure assumes that Host B cannot reach Host A and that a disaster of some sort has occurred on Host A that requires Host B to take over operations for Host A.

Host A must be out of service and the connections to all of its collectible network entities must be dropped so that they can be started on Host B. This means that the NTM application must NOT be running on Host A.

Notes:

1. Before a disaster occurs and as part of normal operations, make sure that the record base, and database, are configured correctly on all hosts.
2. Because this procedure must be done during a disaster situation, we recommend that the audits portion be executed only when necessary; this should reduce any performance degradation.

This procedure prompts you to start an exception printer for the failed Host A.

Instructions

Follow these steps to take over operations from a failed host:

1 Log in to Host B as `root`

2 Log in as `nmadm`

3 Enter `bdr_takeover` *`host_name`*. The *`host_name`* variable identifies the host for which operations are taken over, for example, Host A.

> **Result:** All of the collectible network entities that belonged to Host A and were active, are activated so that data collection can begin on Host B.
>
> Data collection will not begin for these entities until the takeover procedures are completed. Periods of data may be lost for these entities because of this delay. The data collection for the collectible network entities for Host B is not affected.

4 In response to the prompt "`Do you wish to enable/disable an exception/line printer (y/n)?`"

- enter `y` if you want to enable an exception printer at this time and then enter `1` to actually enable the printer.
- enter `n` if you do not want to enable an exception printer at this time.

Result: Entering `y` allows you to enable an exception printer, which begins to print exception reports from the failed host.

5 After the `bdr_takeover` command is completed, determine whether audits should be run on the entities that have been taken over from Host A.

Hint: One reason to run audits (from Host A) on these new entities is if the communication between the two machines was lost for a time before Host A went down and work was being done on Host A that might not have been transferred to Host B.

Important! Under normal circumstances, this step should not be necessary.

6 If it is determined that audits are necessary, log in to Host B using a login that allows viewing of the partition for Host A only and then enter `audit` *`offices`*

Hint: Make sure you are in the partition for which you want to execute the audit.

7 If you executed the `audit all all` command in Step 5, enter `local_audit`

Result: The `local_audit` (Feature 86, "Local Audit Data Restoration") command populates the database using the *Linux* system audit result files that have been backed up from the primary host. `local_audit` does not access any of the entities or other hosts.

Hint: The audit information for a backup host is populated in the database only if the Linux audit result files for the backup host exist on this host.

8 At the end of the next data collection interval, data previously collected from the entities by Host A will be collected by Host B.

END OF STEPS

□

Taking over operations — DCC or TCP/IP

Overview

Purpose

The following procedures should be performed when a host (referred to here as Host B) is to take over the functionality of a DCC or TCP/IP connected office from another host (Host A) that has failed. When this procedure is completed, Host B takes over the data collection and network management operations for the specified DCC or TCP/IP connected office.

Before you begin

Before a disaster occurs and as part of normal operations, make sure that the record base, and database, are configured correctly on all hosts.

Because this procedure must be done during a disaster situation, we recommend that the audits portion be executed only when necessary; this should reduce any performance degradation.

Contents

This section contains the following topics:

□

Taking over operations — DCC

Purpose

This procedure takes over one DCC and the associated offices below it.

Instructions

Follow these steps to take over operations from a DCC:

1 Log in to Host B as `nmadm`

2 Enter `bdr_takeover` *`dcc_name`*. The *`dcc_name`* variable must identify an DCC for which Host B is secondary and which has the proper link configured to allow takeover.

Result: The DCC entity and all collectible entities associated with it will be placed in takeover mode.

3 Check for any instructions on commands that may have to be run manually.

4 After the `bdr_takeover` command is completed, use the `linkstat` command to verify that the *`dcc_name`* is in takeover mode.

5 Enter `act` *`dcc_name`*

6 Verify that the DCC is active before proceeding to Step 7.

7 Enter `act_dcc` *`dcc_name`*

Result: The `act_dcc` command activates the DCC and its respective end offices. Data collection does not begin for these entities until this command is executed.

8 If it is determined that an audit is necessary, then enter `audit` *`dcc_name`* `all`

Important! Before you execute the `audit` command, make sure you are in a partition that can see this DCC.

Result: At the end of the next data collection interval, data previously collected from *dcc_name* by Host A will be collected by Host B.

END OF STEPS

□

Taking over operations — TCP/IP connected switch

Purpose

This procedure takes over one TCP/IP connected switch.

Instructions

Follow these steps to take over operations from a TPC/IP connected switch:

1 Log in to Host A as `nmadm`.

2 If this a failure situation, proceed to Step 4.

Example: Examples of non-failure situations in which you might want to perform this procedure would be a planned facility outage during maintenance, scheduled downtime for maintenance on another NTM, etc.

3 Enter `deact` to deactivate the network element.

Reference: "deact" (p. 11) in the *Input Commands Guide*

4 Log in to Host B as `nmadm` or have `snm` group permissions.

5 Enter `bdr_takeover` *`TCP_name`*. The *`TCP_name`* variable identifies the TCP/IP connected office switch for which operations are taken over, for example, `office_TCP1`.

Result: The collectible network entity that belonged to another host must be activated so that data collection can begin on Host B for this TCP/IP connected switch office.

Data collection will not begin for this entity until the takeover procedures are completed. Periods of data may be lost for this entity because of this delay. The data collection for the collectible network entities for Host B are not affected.

6 After the `bdr_takeover` command is completed, determine whether audits should be run on this entity.

Hint: One reason to run audits is if communications were down between this machine and the machine that the switch was originally on.

7 If it is determined that audits are necessary, enter `audit` *`TCP_name`* `all`

Important! Before you execute the `audit` command, make sure you are in the partition for which this office is defined.

Result: At the end of the next data collection interval, data previously collected from another host for this entity will be collected by Host B.

END OF STEPS

□

Taking over operations — Non-failed host

Purpose

The following procedure should be performed when a host (referred to here as Host B) must take over the functionality of another host (referred to here as Host A). When this procedure is completed, Host B takes over the data collection and network management operations for Host A.

Host A must be out of service and the connections to all of its collectible network entities must be dropped so that they can be started on Host B. This means that the NTM application must NOT be running on Host A. Connectivity to Hosts A's DCC's and *4ESS* offices should be verified before taking over operations.

Before you begin

Before a disaster occurs and as part of normal operations, make sure that the record base, and database are configured correctly on all hosts.

Instructions

Follow these steps to take over operations from a non-failed host:

1. Log in to Host A as `root`

2. Log in to Host B as `root`

3. Verify Host B is available for BDR by using the `linkstat` `typ=nms`

   Reference: "linkstat" (p. 9) in the *Input Commands Guide*

4. Log in as `nmadm`.

   Hint: The `bdr_takeover` *issued in Step 7 will connect all DCC's associated with Host B to Host A. Incremental transfer of DCC's maybe more desirable. For incremental transfer of DCC's, use Step 7; for complete DCC's transfer proceed to Step 7.*

5. Enter `bdr_takeover` *`dcc_name`*

6 For incremental transfer, repeat this step for each DCC. User's may need to execute the `act_dcc` if data collection fails to be restored.

7 Enter `bdr_takeover` *`host_name`*. The *`host_name`* variable identifies the host for which operations are taken over, for example, Host A.

Result: All of the collectible network entities that belonged to Host A are activated so that data collection can begin on Host B.

Data collection will not begin for these entities until the takeover procedures are completed. Periods of data may be lost for these entities because of this delay. The data collection for the collectible network entities for Host B is not affected.

8 In response to the prompt "Do you wish to enable/disable an exception/line printer (y/n)?"

- enter `y` if you want to enable an exception printer at this time and then enter `1` to actually enable the printer.
- enter `n` if you do not want to enable an exception printer at this time.

Result: Entering `y` allows you to enable an exception printer, which begins to print exception reports from the failed host.

9 After the `bdr_takeover` command is completed, determine whether audits should be run on the entities that have been taken over from Host A.

Hint: One reason to run audits (from Host A) on these new entities is if the communication between the two machines was lost for a time before Host A went down and work was being done on Host A that might not have been transferred to Host B. Under normal circumstances, this step should not be necessary.

10 If it is determined that audits are necessary, log in to Host B using a login that allows viewing of the partition for Host A only and then enter `audit` *`offices`*

Hint: Make sure you are in the partition for which you want to execute the audit.

11 If you executed the `audit all all` command in Step 5, enter `local_audit`

Result: The `local_audit` command populates the database using the *Linux* system audit result files that have been backed up from the primary host. `local_audit` does not access any of the entities or other hosts.

Hint: The audit information for a backup host is populated in the database only if the Linux audit result files for the backup host exist on this host.

12 At the end of the next data collection interval, data previously collected from the entities by Host A will be collected by Host B.

END OF STEPS

□

Synchronizing record base files with another host

Purpose

After a host fails, a backup host takes responsibility for the failed host's record base files. After the failed host has been repaired, you may use this procedure to make sure that the record base files are synchronized with the backup host. This procedure will synchronize the primary record base partitions on this host from a backup host.

⚠ **CAUTION**

Because this procedure overwrites the files of the host on which it is executed, it is recommended that the record base be backed up first with the procedures given in Chapter 5, "Backing Up and Restoring the System".

Instructions

Follow these steps to synchronize record base files with another host:

1 Log in as `nmadm`.

2 Type `/nm/sys/bdr_sync` *`from_host`*.

Result: Synchronizes files in the primary record base partitions on this host with those on the host specified by *`from_host`*.

Reference: "bdr_sync" (p. 13) in the *Input Commands Guide*

END OF STEPS

□

Returning operations to the original host

Purpose

The following procedure should be executed when a host (Host B) that has taken over operations for a failed host (Host A) with the `bdr_takeover` command must return responsibility for those operations to the original host. As part of this procedure, Host B returns to its backup status so that Host A can start to collect data and manage the network again.

This procedure should be executed when there is little activity on the network and it is not critical if data collection is lost for a short time.

> **Important!** If you cannot perform this procedure at the time of the switchback because of a system failure on the host currently in takeover mode, you may postpone the execution of the `bdr_switchbk` command until the host is operational. Network elements still can be taken over by the other host.

This procedure prompts you to specify whether you want to disable an exception printer that has been enabled for Host A.

Instructions

Follow these steps to return operations to the original host:

1 Make sure that all problems on Host A that required the takeover have been corrected and that Host A is at run level 3. If Host A is not at run level 3, execute `init 3`

2 If Host A has been out of service for a long time and Host B has made many changes to Host A's record base, back up the record base on Host A and then execute the `bdr_sync` command on Host A to synchronize its primary record base partitions with those on Host B.

> **Result:** The `bdr_sync` command only synchronizes the primary partition on Host A.

3 If you executed `bdr_sync` in Step 2, execute `recreate` now to update the record base files copied from the other host.

4 Log in to Host B as `root`

5 Enter `deact` for all the links that are defined for Host A entities that are to be switched back to Host A.

Result: Host B must relinquish its operation on the part of the network normally managed by Host A. It also must deactivate its data collection links before Host A can activate its data collection links and start to collect data.

6 Log in as `nmadm` or have `snm` permissions.

Result: The `bdr_switchbk` issued in Step 7 will connect all DCC's associated with Host B to Host A. Incremental transfer of DCC's maybe more desirable. For incremental transfer of DCC's use Step 7, for complete DCC's transfer proceed to Step 9.

7 Enter `bdr_switchbk` *`dcc_name`*

8 For incremental transfer, repeat this step for each DCC. User's may need to execute the `act_dcc` if data collection fails to be restored.

9 Still on Host B, execute `bdr_switchbk` *`host_name`*. The variable *host_name*, in this example, would be Host A.

Result: The part of the network normally managed by Host A is deactivated on Host B.

Important! If Host B is not operational, you may skip this step. However, you must perform it as soon as Host B becomes operational.

10 In response to the prompt "`Do you wish to enable/disable an exception/line printer (y/n)?`"

- Enter `y` if you want to disable the exception printer if one is running for Host A and then enter `2` to actually disable the printer.
- Enter `n` if you do not want to disable the exception printer.

11 If you enabled an exception printer when you took over the host, you should disable it at this time.

12 On Host A, enter `startsys` to start the NTM application and data collection.

> **Important!** Data collection is ***not*** done during the interval between execution of `bdr_switchbk` on Host B and `startsys` on Host A.

13 Use the `linkstat` command to verify that appropriate network entities are shown as activated. If they are not active, then use the `act` command to activate the entities before moving on to the next step.

Hint: This step is necessary because conditions may exist whereby the proper network entities are not in the correct activation status at a given time.

14 If you have Feature 86, “Local Audit Data Restoration”, enter `local_audit`

> **Result:** The `local_audit` command populates the database using the *Linux* system audit result files that have been backed up from the primary host. `local_audit` does not access any of the entities or other hosts.

Hint: The audit information for a backup entity is populated in the database only if the Linux audit result files for the entity exist on this host.

15 Enter `audit` all tg.

> **Result:** By running `audit` all tg before the next steps, trunk group reference data will be created. As soon as the office data for a trunk group is created by subsequent audits, trunk groups will begin to display data for network surveillance.

16 On Host A, enter `audit all all` to ensure that all data is synchronized with the data in the offices.

END OF STEPS

□

Returning operations to original host — DCC or TCP/IP

Overview

Purpose

Use the following procedure to return responsibility for a single DCC or TCP/IP connected switch from the takeover host to the original host. As part of this procedure, the takeover host returns to its backup status on the network entity so that the original host can start to collect data and manage this entity again.

Contents

This section contains the following topics:

□

Returning operations to original host — Single DCC

Instructions

Follow these steps to return operations to the original host for a single DCC:

1 Log in to Host B as `nmadm`

2 Execute `bdr_switchbk` *`dcc_name`*. The variable *`dcc_name`* is a DCC office that is normally configured to collect data on Host A.

> **Result:** This DCC office is deactivated on Host B so that Host A can begin to collect data from it again.

Hint: If Host B is not operational, you may skip this step. However, you must perform it as soon as Host B becomes operational.

3 Make sure that the specified *`dcc_name`* is deactivated before continuing.

4 When the `bdr_switchbk` command is complete, enter `deact_dcc` *`dcc_name`*.

> **Result:** When this command is completed, all of the end offices under this DCC will be deactivated.

5 Check for any instructions on commands that may have to be run manually.

> **Important!** Data collection is ***not*** done during the interval between execution of `bdr_switchbk` on Host B and this command on Host A.

6 On Host A, enter `audit` *`dcc_name`* `all` to ensure that all data is synchronized for this office.

END OF STEPS

□

Returning operations to original host — TCP/IP

Instructions

Follow these steps to return operations to the original host for a TCP/IP connected switch:

1 Log in to Host B as `nmadm`

2 On Host B, execute `bdr_switchbk` *`TCP_name`*. The variable *`TCP_name`*, in this example, would be the name of the TCP connected switch office (in takeover mode) that is to be returned to Host A.

This TCP connected switch office is normally managed by Host A. It must be deactivated and taken out of takeover mode on Host B.

Hint: If Host B is not operational, you may skip this step. However, you must perform it as soon as Host B becomes operational.

3 Log in to Host A as `nmadm`.

4 On Host A, enter `act` *`TCP_name`* to activate data collection.

The link must be connected before data collection can begin.

> **Important!** Data collection is ***not*** done from the time the `bdr_switchbk` command is executed for this *TCP* connected switch office on Host B until this step is completed and the link to the *TCP connected* switch has been established.

5 On Host A, enter `audit` *`TCP_name`* `all` to ensure that the NTM database is synchronized with the data from this office.

> **Important!** This step is recommended if communication between Host A and Host B has been down for an extended time.

END OF STEPS

□

Backing up the host with BDR active

Purpose

When commands such as `create`, `dbtest`, or `bdr_commit` are executed while BDR is active, the commands will perform the following additional tasks to back up any changes on the backup host:

> **Important!** BDR must be available and active on all hosts for the backup procedure to work properly.

- Commands will check the status of the desired record base files on this host (for example, status of the "/musr/rb/inms/inms" file when `create office` is run).

  Backup procedures are permitted only for global record base files in the PRIMARY state (see the "Changing global record base file state — inactive" (p. 35)) or other record base files located in a primary record base partition (as defined in the inms record base file).
- The status of BDR and desired record base files then will be checked on the backup host.

  Back up procedures will be permitted on the backup host only for global record base files in the BACKUP state (see the "Changing global record base file state — inactive" (p. 35)) or other record base files located in a backup record base partition (as defined in the inms record base file).
- If the conditions mentioned above are true, the desired record base files will be copied to the backup host. The user must have write permissions on the backup hosts for the affected record base files.
- If the files are copied successfully, the command (such as `create`) will be executed on the backup host for the desired record base files.

Figure

Figure 4 provides an example of the output for the `create office` command.

Figure 4 create office command output

```
$ create office clmboh0001t
Have you run dbtest on office(s)? (yes, no)
y
  IP
Starting create (pid 15855) at Mon Sep 14 14:55:06 1992

Initializing clmboh0001t
Creating clmboh0001t from /musr/rb
       Trunk group file does not exist
       Pool trunk group file does not exist
       Adding 11 domains to office
       Adding 1 TTO thresholds to office
Creating inms
Finished create (pid 15855) at Mon Sep 14 14:55:53 1992

Copying /musr/rb/office/clmboh0001t to cbnmsb, please wait...

Copying /musr/rb/tg/clmboh0001t to cbnmsb, please wait...

Copying /musr/rb/domain/clmboh0001t to cbnmsb, please wait...

Copying /musr/rb/tto/clmboh0001t to cbnmsb, please wait...

Executing /nm/sys/bdr_create on cbnmsb, please wait...
  IP
Starting bdr_create at Mon Sep 14 14:55:41 1992
Initializing clmboh0001t
Creating clmboh0001t from /musr/snw/pbso/rb
       Trunk group file does not exist
       Pool trunk group file does not exist
       Adding 11 domains to office
       Adding 1 TTO thresholds to office
Creating inms
Finished bdr_create at Mon Sep 14 14:55:43 1992
```

□

Backing up the DCC_Alias file

Instructions

Follow these steps to back up the “dcc_alias” file to all backup hosts.

1 Enter `bdr_chgstat -p /musr/rb/dcc_alias`

Result: Changes the state of *“dcc_alias”* file to primary.

2 Edit the *“dcc_alias”* file and make the desired changes.

3 Enter `bdr_commit /musr/rb/dcc_alias`

Result: Backs up the file to all backup hosts.

4 Enter `bdr_chgstat -b /musr/rb/dcc_alias`

Result: Changes the state of *“dcc_alias”* file to backup.

END OF STEPS

References

Chapter 4, “Data Collection Concentrator Alias File” in the *Record Base Administration Guide*

□

13 ARC Administration

Overview

Purpose

ARC is optional. It is available only if Feature 106, "Active Request Controller" has been purchased.

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
Starting ARC	5 minutes	X	
Stopping ARC	5 minutes	X	

Contents

This chapter contains the following topics:

□

How does ARC work?

Overview

ARC supports program-level connections to external processes via a LAN (Local Area Network) TCP/IP-based connection for the purpose of processing multiple SQL (Structured Query Language) data requests to a data base in the NTM host. With ARC, the requested data is returned in one-third to one-half the time required by the `demand` and `fmltoasc` commands.

Benefits

The benefit of using the ARC service is an overall increase in the throughput of the SQL requests from an external, non-NTM process. This is accomplished by having ARC act as a daemon process which is continuously up and ready to handle requests. Unlike the normal use of `demand` and `fmltoasc`, ARC is not recreated for each new request. This eliminates most of the overhead associated with the startup of the current `demand` and `fmltoasc` processes on a per request basis. The elimination of this overhead decreases the response time and allows for an increased volume of requests without a significant increase in the use of NTM host resources.

Functionality

The ARC service is handled by a single process that combines the functionality of the `demand` and `fmltoasc` commands. An ARC process is created from an external system as follows:

1. The external system logs in to NTM.
2. The `start_arc` command is issued from the external system.
3. The command responds with a socket number and a process ID number.
4. The SQL queries are run with the same permissions as the login that started the ARC process.

If the external system wants to kill the ARC process, the `stop_arc` command is used. The argument to this command is the process ID returned when the process was created with the `start_arc` command.

Reference: An *Interface Programmer's Guide* is available from the NTM development group. Contact your site manager for more information.

□

Starting ARC

Purpose

To start an ARC session, the user must log on to NTM and execute the `start_arc` command. This command accepts the same command line arguments as those accepted by `fmltoasc`

Important! ARC will not accept SQL queries of 1024 bytes or longer.

Syntax

The command syntax is

```
start_arc [-prel],[-f strg],[-m strg],[-s char], [-w char],[-n char],[-c
char], [-i strg], [-t <n>]
```

Parameters

`-p` Print the data in the form <fieldname>=<value>.

`-r` Print only the retrieved fields, that is, those from the select clause of the SQL file. The default is to print all the fields contained within the fielded buffer.

`-e` Print the value and exception level for calculated fields. The default is to print only the value.

`-l` Print the label associated with the select clause. The label is optional in the SQL file, therefore this option may display a null string.

`-f <strg>` Use the string <strg> as the field delimiter string. The default delimiter string is the blank.

Important! Do not use the `-f` option with the `-w` and/or `-n` options because the `-f` option takes precedence.

`-m <strg>` Use the string <strg> as the message delimiter string. The default delimiter string is a newline.

`-s <char>` Use the character <char> as the subfield delimiter character. The default delimiter character is a blank. This option is used when a field is made up of several subfields.

`-n <char>` Use the character <char> as the delimiter character before a number. The default delimiter character is a blank.

`-c <char>` Use the character <char> as the delimiter between fields in calculated fields. The default delimiter character is a blank.

`-i <strg>` Use the string <strg> as the invalid data string. The default invalid data string is “-1”.

`-t<n>` Use the number <n> as the time format definition as shown here:

- n = 1 *Linux* system date format
- n = 2 hour and minute
- n = 3 date, hour and minute
- n = 4 hour, minute, and second (default)
- n = 5 date, hour, minute, and second

System responses

After you have run the command, `start_arc` will determine if the ARC feature lock is set. If ARC is locked (i.e. has not been purchased), an error message is returned, and no ARC process is started.

Next, `start_arc` determines if the maximum number of active ARC sessions has already been reached. If so, an error message is printed, and start_arc terminates without starting an ARC process.

Important! No more then 3 ARC sessions can be run at once.

If the maximum number of active ARCs has not been reached, then start_arc starts an ARC process. It then prints out both the process ID of the running ARC process and the socket with which it is associated. The external system uses the socket number for sending SQL queries to the ARC process. The process ID is used when ARC is to be terminated. Once the ARC process has been started and the process ID and the socket number have been printed, the `start_arc` command dies.

Instructions

Follow these steps to start the ARC process.

1 Log in to NTM

Result: The group associated with the user determines which subnetwork restrictions, if any, will be enforced on the queries.

2 Execute the `start_arc` command.

Hint: The command accepts the same command line arguments as are currently accepted by `fmltoasc`.

Result: The system prints both the process ID of the running ARC process and the socket with which it is associated.

END OF STEPS

□

Stopping ARC

Purpose

To stop an ARC session, the user must log in to NTM and execute the `stop_arc` command.

Syntax

The command syntax is

```
stop_arc <pid>
```

Parameters

`<pid>`	process number of the ARC process to be killed

System responses

If that is a process number of an active ARC process and the user has the necessary permission to kill that process, the process is killed, and the `stop_arc` command dies.

Instructions

Follow these steps to stop the ARC process.

1 Log in to NTM

Hint: An ARC process can be stopped only by the user ID used to start it, or by `root`.

2 Execute the `stop_arc` *`<pid>`* command.

Result: The process is killed.

END OF STEPS

□

14 Capacity and Usage Reporting

Overview

Purpose

Feature 130, "Capacity and Usage Reporting" enables NTM personnel to collect capacity and performance data and to obtain reports of performance data on a daily basis or upon request. With this feature, NTM personnel will be able to monitor the usage of the significant application software components running on the host computer and their associated use of host computing resources. The following components make up this feature:

- Data collection — The data collection component collects and stores usage and performance information. It is transparent to users, but it forms the basis for the reports.
- Reports — The reports component generates reports that can be scheduled in cron to run daily, or requested by users for a given interval within the day. Reports are run on demand only.

Contents

This chapter contains the following topics:

□

Types of data collected

Overview

The types of data collected for the reports consist of the following general categories.

1. ***Network Elements in the Database*** — For example: the number of DCCs (Data Collection Concentrators), hosts, and switches; the number of trunk groups; the number of trunk group calculations, etc.
2. ***User Process Data*** — For example: audits, controls, ongoing, etc.
3. ***CPU Usage*** — For example: statistics on the activity level in the system on an hourly basis
4. ***System Resources Usage*** — For example: Tuxedo database usage.

□

Reports

Types of reports

Users create reports by using the perfrep command. There are two types ofreports that can be generated.

1. Daily report -- Prints data for the previous day (by default). This consists of the NTM data for the 24-hour period. The Daily Report contains information for a single 24-hour period, previous to the current day. The report shows this information in three 8-hour sections.
2. Summary report -- Prints data for the current day (by default). This consists of the NTM data for the 24-hour period.

Daily report

The Daily report contains summary-level information for a single 24-hour period previous to the current day. The report output has three 8-hour sections. Data for the report must be available in NTM for this report to be successful. You cannot use the endtime or starttime arguments for this type of report.

Use the following command line to request a daily report:

```
perfrep [report=daily date=date format=format] [-h]
```

For more specific information on the `perfrep` command and its valid arguments, see the *Input Commands Guide*.

Summary report

The Summary report contains the same kind of information as the daily report, but for a user-specified period of time. You can use the date argument to specify the day (mm/dd) for the report and the starttime argument to indicate the starting and ending times for the report in whole-hour increments. If you do not use these arguments, the day defaults to the current day, the starttime defaults to 0:00, and the ending time defaults to 23:00.

Use the following command line to request a summary report:

```
perfrep report=summary [date=date starttime=starttime
  endtime=endtime format=format] [-h]
```

Viewing reports

For all report types, you can use the `format=data` argument on the command line to produce a data version of the output to use in scripts or on spreadsheets. This option causes the output to be formatted with commas as delimiters between the data fields instead of in table format. If you obtain the report in data format, you can then download it into a PC spreadsheet package and manipulate the data to produce graphs, bar charts, and other types of output that may be useful to you.

Scheduling reports

You can schedule the daily report to run out of cron daily and store the results in files. Data is retained for seven days so that you can run Friday's report on Monday if you wish.

Report permission

Normally only a member of the snm user group can run reports. However, the system administrator can change the permissions for the `perfrep` command in the *"/nm/etc/permissions"* file and assign any user group permission to run the command.

System limitations

To minimize the impact of Feature 130 on the resources of the system, you should run no more than one or two `perfrep` commands a day.

□

Interpreting reports

Overview

Purpose

This section provides information about interpreting reports, along with examples of the different sections that comprise a report.

Sections

Whether you run a daily report or a summary report, the sections of the report are the same.

Data keys

The output data files consist of a data item followed by a data key. The key is one of three characters.

IF the data key is a …	THEN …
(blank space)	the data is good.
#	the data is missing.
*	the collection process is initialized or missing a timed entry.

Important! If the key is either a * or a #, then the data is suspect.

Missing data

An expected occurrence of the missing data occurs when accounting is routinely turned off each night. This causes the CPU usage measurements to report that data is missing.

Contents

This section contains the following topics:

□

Network Elements in the Database

Purpose

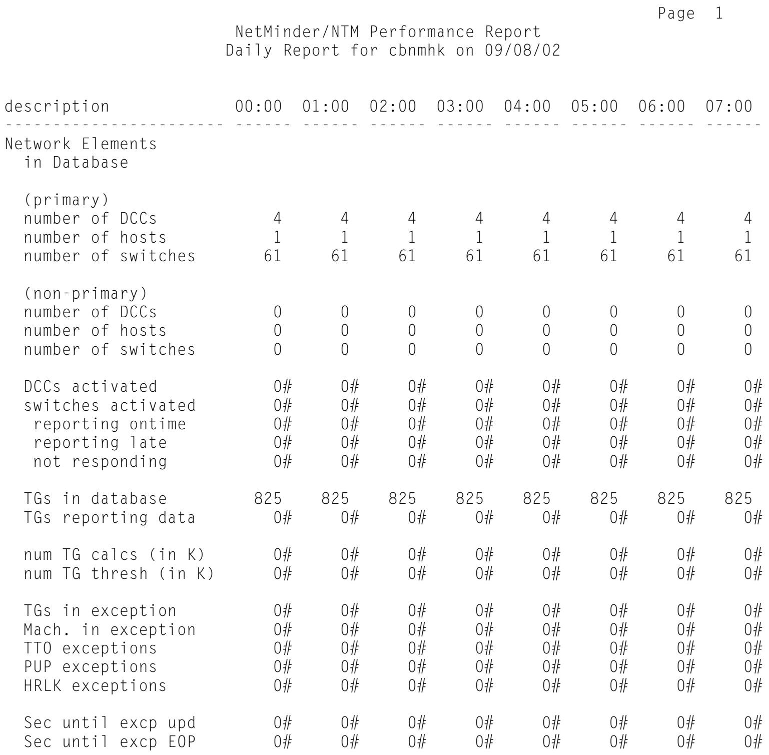
A sample of the Network Elements in the Database section of the report is shown in Figure 1. It reports on the counts shown in the example for an 8-hour time period.

The statistics for the DCCs, hosts, and switches are collected and stored once for each 24-hour period. All other statistics are collected and stored every five minutes and then averaged.

Figure

Table 1, which follows Figure 1, lists the labels found in this section of the report and a description of the label.

Figure 1 Sample daily report — Network Elements in Database section



```
                                                                   Page  1
                       NetMinder/NTM Performance Report
                      Daily Report for cbnmhk on 09/08/02


description             00:00  01:00  02:00  03:00  04:00  05:00  06:00  07:00
----------------------- ------ ------ ------ ------ ------ ------ ------ ------
Network Elements
  in Database

  (primary)
  number of DCCs            4      4      4      4      4      4      4      4
  number of hosts           1      1      1      1      1      1      1      1
  number of switches       61     61     61     61     61     61     61     61

  (non-primary)
  number of DCCs            0      0      0      0      0      0      0      0
  number of hosts           0      0      0      0      0      0      0      0
  number of switches        0      0      0      0      0      0      0      0

  DCCs activated           0#     0#     0#     0#     0#     0#     0#     0#
  switches activated       0#     0#     0#     0#     0#     0#     0#     0#
   reporting ontime        0#     0#     0#     0#     0#     0#     0#     0#
   reporting late          0#     0#     0#     0#     0#     0#     0#     0#
   not responding          0#     0#     0#     0#     0#     0#     0#     0#

  TGs in database         825    825    825    825    825    825    825    825
  TGs reporting data       0#     0#     0#     0#     0#     0#     0#     0#

  num TG calcs (in K)      0#     0#     0#     0#     0#     0#     0#     0#
  num TG thresh (in K)     0#     0#     0#     0#     0#     0#     0#     0#

  TGs in exception         0#     0#     0#     0#     0#     0#     0#     0#
  Mach. in exception       0#     0#     0#     0#     0#     0#     0#     0#
  TTO exceptions           0#     0#     0#     0#     0#     0#     0#     0#
  PUP exceptions           0#     0#     0#     0#     0#     0#     0#     0#
  HRLK exceptions          0#     0#     0#     0#     0#     0#     0#     0#

  Sec until excp upd       0#     0#     0#     0#     0#     0#     0#     0#
  Sec until excp EOP       0#     0#     0#     0#     0#     0#     0#     0#
```

Table

Table 1 describes the labels found in Figure 1.

Table 1 Network Elements in the Database section

Label	Description
(Primary) Number of DCCs	Number of DCCs in the database where this is the primary partition
(Primary) Number of hosts	Number of hosts in the database where this is the primary partition
(Primary) Number of switches	Number of switches in the database where this is the primary partition
(Non-primary) Number of DCCs	Number of DCCs in the database where this is the backup partition
(Non-primary) Number of hosts	Number of hosts in the database where this is the backup partition
(Non-primary) Number of switches	Number of switches in the database where this is the backup partition
DCCs activated	Number of data collection concentrators
Switches activated	Number of offices polled for 5-minute data
Reporting ontime	Number of offices reporting ontime (before the end of exception update interval)
Reporting late	Number of offices reporting after end of exception update but before end of period
Not responding	Number of offices not reporting before end of period
TGs in database	Number of TGs in the database in all partitions
TGs reporting data	Number of TGs for which data is reported
Num TG calcs (in K)	Number of TG calculations performed by exceptions in 1000's
Num TG thresh (in K)	Number of TG thresholds performed by exceptions in 1000's
TGs in exception	Number of TGs with exceptions
Mach. in exception	Number of machines with exceptions
TTO exceptions	Transmitter timeout exceptions
PUP exceptions	Peripheral unit processor exceptions
HRLK exceptions	Host remote link exceptions
Sec until excp upd	Average length of the exception update interval in seconds
Sec until excp EOP	Average length of period in seconds

□

User Process Data

Purpose

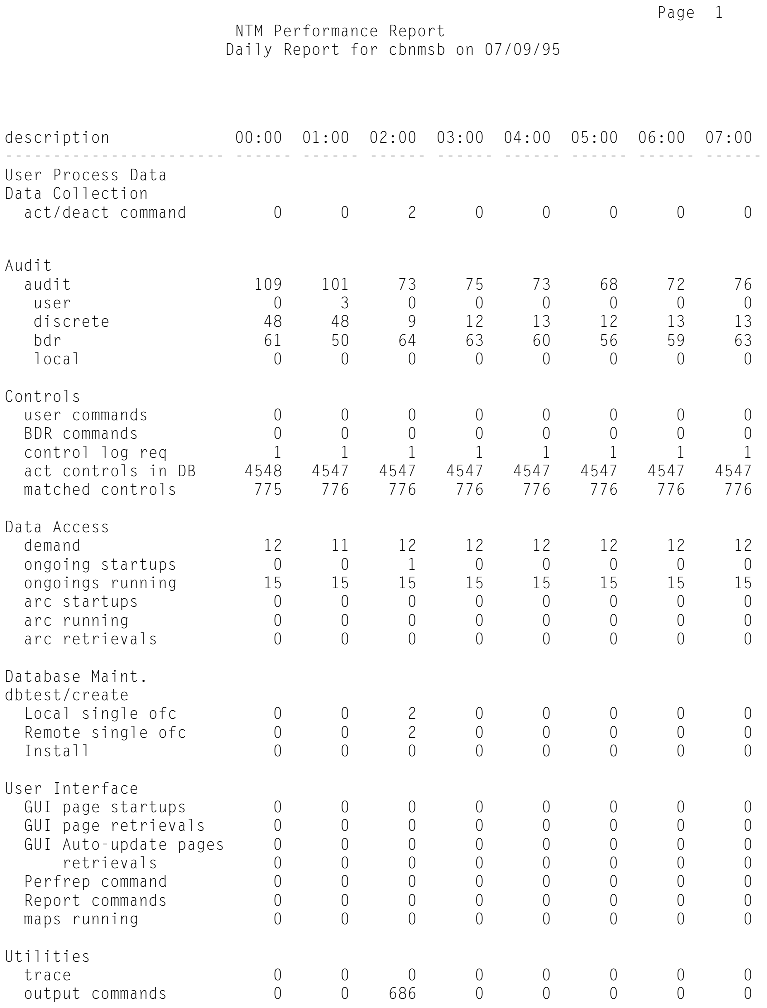
A sample of the User Process Data section of the report is shown in Figure 2. It reports on various user activities.

The statistics in this section are incremental counts for each of the activities.

Figure

Table 2, which follows Figure 2, describes the labels found in this section of the report, the maximum or expected value for that label, and a description of the label.

Figure 2 Sample daily report — User Process Data section



```
                                                                    Page  1
                        NTM Performance Report
                       Daily Report for cbnmsb on 07/09/95



description              00:00  01:00  02:00  03:00  04:00  05:00  06:00  07:00
----------------------- ------ ------ ------ ------ ------ ------ ------ ------
User Process Data
Data Collection
  act/deact command          0      0      2      0      0      0      0      0


Audit
  audit                    109    101     73     75     73     68     72     76
   user                      0      3      0      0      0      0      0      0
   discrete                 48     48      9     12     13     12     13     13
   bdr                      61     50     64     63     60     56     59     63
   local                     0      0      0      0      0      0      0      0

Controls
  user commands              0      0      0      0      0      0      0      0
  BDR commands               0      0      0      0      0      0      0      0
  control log req            1      1      1      1      1      1      1      1
  act controls in DB      4548   4547   4547   4547   4547   4547   4547   4547
  matched controls         775    776    776    776    776    776    776    776

Data Access
  demand                    12     11     12     12     12     12     12     12
  ongoing startups           0      0      1      0      0      0      0      0
  ongoings running          15     15     15     15     15     15     15     15
  arc startups               0      0      0      0      0      0      0      0
  arc running                0      0      0      0      0      0      0      0
  arc retrievals             0      0      0      0      0      0      0      0

Database Maint.
dbtest/create
  Local single ofc           0      0      2      0      0      0      0      0
  Remote single ofc          0      0      2      0      0      0      0      0
  Install                    0      0      0      0      0      0      0      0

User Interface
  GUI page startups          0      0      0      0      0      0      0      0
  GUI page retrievals        0      0      0      0      0      0      0      0
  GUI Auto-update pages      0      0      0      0      0      0      0      0
      retrievals             0      0      0      0      0      0      0      0
  Perfrep command            0      0      0      0      0      0      0      0
  Report commands            0      0      0      0      0      0      0      0
  maps running               0      0      0      0      0      0      0      0

Utilities
  trace                      0      0      0      0      0      0      0      0
  output commands            0      0    686      0      0      0      0      0
```

Table

Table 2 describes the labels found in Figure 2.

Table 2 User Process Data section (Sheet 1 of 2)

Category	Label	Maximum or Expected Value	Description
Data collection	act/deact command	NA	Number of `act/act_dcc/deact/deact_dcc` commands executed
Audit	audit	370	Total number of audits run of all types
	users	36	Number of user requested audits run
	discrete	50	Number of discrete triggered audits run
	bdr	85	Number of BDR audits run
	local	200	Number of local audits run
Controls	user commands	100	Number of control commands input by the user
	BDR commands	100	Number of control commands input by BDR
	page commands	100	Number of control commands input by pages
	control log req	100	Number of control log requests
	act controls in DB	TBD	Number of active controls in the database
	matched controls	TBD	Number of matched controls in the database
Data Access	demand	36	Number of demand requests
	ongoing startups	*	Number of ongoing requests
	ongoings running	*	Average number of ongoing processes running
	arc startups	NA	Number of `start_arc` requests
	arc running	*	Average number of arc processes running
	arc retrievals	250	Number of arc retrievals
Database Maint - dbtest/create	local single office	10	Number of single office `dbtest/create` initiated on this host
	remote single office	10	Number of single office `dbtest/create` initiated from the remote host
	install	0	Number of `install` commands run

Table 2 User Process Data section (Sheet 2 of 2)

Category	Label	Maximum or Expected Value	Description
User Interface	GUI page startups		Number of GUI pages loaded
	GUI page retrievals		Number of retrievals (Search) from a GUI page
	GUI Auto-update pages		Number of GUI pages in Automatic Update mode
	GUI Auto-update pages retrievals		Number of retrievals while in Automatic Update mode
	`perfrep` command	2	Number of `perfrep` commands requested
	report commands	10	Number of `darpt, firpt, icrpt, ncrpt,` and `oprpt` commands
	maps running		Number of maps running.
Utilities	trace	1	Number of `tracer` commands
	output commands	10	Number of opblock, opcg, opcni, opentref, opents, opentstat, opfhc, ophtr, opnoderef, opntnxcpt, opshm, optab, optgref, optgxcpt, opthresh, optv, and opxref processes

□

CPU Usage

Purpose

A sample of the CPU Usage section of the report is shown in Figure 3. It reports on CPU usage for user processes.

The statistics for this section of the report are obtained from the *Linux* system `acctcom` and `ps` commands. At the end of each hour the `ps` command is run and the data is stored. This data is combined with `acctcom` information to determine the CPU usage for each activity for the specified 1-hour period.

Figure

Table 3, which follows Figure 3, describes the labels found in this section of the report, the maximum or expected value for that label, and a description of the label.

Figure 3 Sample daily report — CPU Usage section

```
                        NTM Performance Report


description             00:00  01:00  02:00  03:00  04:00  05:00  06:00  07:00
----------------------- ------ ------ ------ ------ ------ ------ ------ ------
CPU Usage
Data Collection
  Data collectors           0#     0    353    437    452    429    449    465
  Act/deact                 0#     0      2      0      0      0      0      0

Exception
  EXCP                      9#    10    379    430    416    449    501    502
  EXCPDUMP                  0#    53     48      0     89    230     10     28
  EXCPCPLT                  2#     3      2      2      3      1      3      3

Audit
  processing                0#     0    100    110    109    104    107    117

Controls
  Commands                  0#     0      0      0      0      0      0      0
  Server                    0#     0      2      0      0      0      0      0
  Log                       0#     0     33     33     35     31     29     32
Data Access
  Database retrieval        0#     0     16     12     13     12     11     12
  Demand                    0#     0     19     22     21     18     14     16
  Fmltoasc                  0#     0      0      0      0      0      0      0
  Urwformat                 0#     0      0      0      0      0      0      0
  Ongoing                   0#     0    238    300    293    300    302    298
  DMON                      0#     0    181    186    188    194    195    198
  ARC                       0#     0      0      0      0      0      0      0
GUISRVR                   0#     1      0      0      0      0      0      0
  java                     22#    28     26     26     27     26     25     26
  listen                    0#     0     15      0     39      0      0      0
  map servers               0#     0      0      0      0      0      0      0
  web servers              69#    76     76     75     77     76     74     77

Database Maint.
  Dbtest/create             0#     0      2      0      0      0      0      0
  Install                   0#     0      0      0      0      0      0      0

User Interface
  Auto update               0#     0     45      9      6      9     10     11
  Performance               0#     0     21     10      9     11     10     11

Utilities
  report                    0#     0      0      0      0      0      0      0
  failrep                   0#     0      0      0      0      0      0      0
  OP                        0#     0     41      0      0      0      0      0
  report_xmt                1#     0      0      1      0      1    . 2      0
  oracle                    0#     0      0      0      0      0      0      0
  BrioQuery                 0#     0      0      0      0      0      0      0

Other
```

```
  dbtape                 0#     0      0      0      0      0       0      0
  other processes        0#     0   1018    313    290    498     286    292

LEGEND: # - data is missing       * - data is suspect
```

Table

Table 3 describes the labels found in Figure 3.

Table 3 CPU Usage section (Sheet 1 of 2)

Category	Label	Maximum or Expected Value	Description
Data collection	Data collectors	360	CPU seconds used by DCUP, DCOL_ED, DCOL_QED, DCOL_4E, DCON_FEP, DCOL_NMS, rcv, and RMSRCV processes
	Act/deact	+	CPU seconds used by `act, act_dcc, deact,` and `deact_dcc` commands
Exception	EXCP	3600	CPU seconds used by EXCP process
	EXCPDUMP	3600	CPU seconds used by EXCPDUMP process
	EXCPCPLT	3600	CPU seconds used by EXCPCPLT
Audit	processing	360	CPU seconds used by audit, AUDSRV, and AUDDMP processes
Controls	Commands	+	CPU seconds used by canf, cant, pp, cg, cro, dhtr, ihtr, doc, pplist, ofcovrd, rr, silc, skip str, and total processes
Server	Server	+	CPU seconds used by CTLSRV process
Log	Log	+	CPU seconds used by ctrlog and purglog processes
Data Access	Database retrieval	+	CPU seconds used by DBSRVR process
	Demand	+	CPU seconds used by demand process
	Fmltoasc	+	CPU seconds used by fmltoasc process
	Urwformat	+	CPU seconds used by urwformat process
	Ongoing	+	CPU seconds used by ongoing process
	DMON	+	CPU seconds used by DMON process
	ARC	+	CPU seconds used by start_arc and stop_arc processes

Table 3 CPU Usage section (Sheet 2 of 2)

Category	Label	Maximum or Expected Value	Description
	GUISRVR	+	CPU seconds used by GUISRVR process
	java	+	CPU seconds used by java process
	listen	+	CPU seconds used by listen process
	map servers	+	CPU seconds used by map servers process
	web servers	+	CPU seconds used by web servers
Database Maint.	Dbtest/create	360	CPU seconds used by create, dbtest, and thresh processes
	Install	+	CPU seconds used by installdb process
User Interface	Performance	70	CPU seconds used by perfrep and perfcol processes
Utilities	report	+	CPU seconds used by darpt, firpt, icrpt, ncrpt, and oprpt processes
	failrep	+	CPU seconds used by failrep command
	OP	+	CPU seconds used by opblock, opcg, opcni, opentref, opents, opentstat, opfhc, ophtr, opnoderef, opntnxcpt, opshm, optab, optgref, optgxcpt, opthresh, optv, and opxref processes
	report_xmt	+	CPU seconds used by report_xmt process
	oracle	+	CPU seconds used by oracle software process
	BrioQuery	+	CPU seconds used by BrioQuery software process.
Other	dbtape	+	CPU seconds used by dbtape process
	Other processes	+	CPU seconds used by all other processes

□

System Resource Usage

Purpose

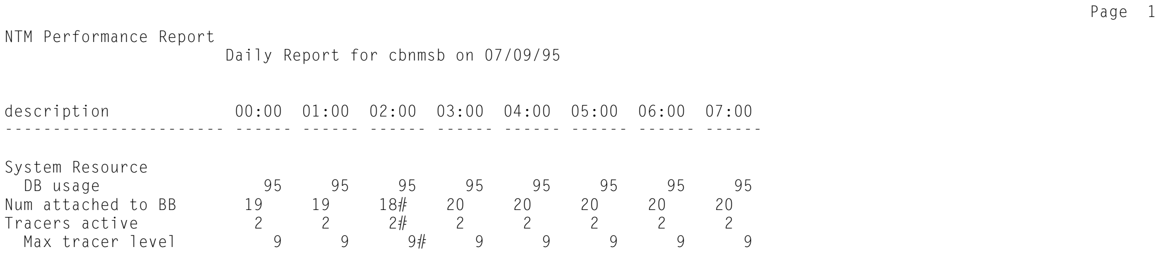
A sample of the System Resource Usage section of the report is shown in Figure 4. It reports on system resources to allow the user to determine if the system is nearing capacity.

The statistics for this sections of the report are reported as percentages or raw counts. The Ethernet and tracer activities are reported as raw counts. All other statistics are reported as a percentage of capacity.

Figure

Table 4, which follows Figure 4, describes the labels found in this section of the report, the maximum or expected value for that label, and a description of the label.

Figure 4 Sample daily report — System Resource section



```
                                                                                                                 Page  1
NTM Performance Report
                       Daily Report for cbnmsb on 07/09/95


description             00:00  01:00  02:00  03:00  04:00  05:00  06:00  07:00
----------------------- ------ ------ ------ ------ ------ ------ ------ ------

System Resource
  DB usage                 95     95     95     95     95     95     95     95
Num attached to BB       19     19     18#    20     20     20     20     20
Tracers active            2      2      2#     2      2      2      2      2
  Max tracer level          9      9      9#     9      9      9      9      9
```

Table

Table 4 describes the labels found in Figure 4.

Table 4 System Resource section

Label	Maximum or Expected Value	Description
DB usage	50	Percent of the database that is used
Num attached to BB the bulletin board	80	Average number of users attached to the bulletin board
Tracers active	+	Average number of tracers active
Max tracer level	+	Average maximum tracer level

□

15 Surveillance Transition to Additional Trunk Groups

Overview

Purpose

This chapter provides background and procedural information related to adding trunk groups for surveillance.

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Setting up DMS 1024 trunk group surveillance — DCC" (p. 5)	1 Hour	X	
"Setting up the database for Feature 264" (p. 7)	1 Hour	X	
"Setting up surveillance for more than 250/500 TGs (TCP)" (p. 9)	1 Hour	X	

Contents

This chapter contains the following topics:

□

Requirements

Features for additional trunk groups

This chapter only applies if you have purchased the following optional features:

- Feature 263, “DMS 100/200 Switch Surveillance of 1024 Trunk Groups Via FEP”
- Feature 264, “DMS 100/200 Switch Surveillance of 1024 Trunk Groups Via TDM”
- Feature 265, “DMS 100/200 Surveillance of 1024 Trunk Groups Via DCOS-2000”
- Feature 283, “Surveillance of 2000 Trunk Groups in a 5ESS Switch”
- Feature 284, “Surveillance of 1024 Trunk Groups in a DMS 100/200 Switch”
- Feature 285, “Surveillance of 1024 Trunk Groups in a DMS 250 Switch”
- Feature 286, “Surveillance of 1024 Trunk Groups in a DMS 500 Switch”
- Feature 341, “Map Alert Restrictions for the Browser-based GUI”
- Feature 355, “Surveillance of 1024 Trunk Groups in a Succession Network Switch Generic SN02”

Prerequisite features

The following features must be purchased for the previously listed optional features to function:

- Feature 195, “System Hardware HP Platform and Performance Upgrade”
- Feature 215, “DMS 250 Switch Support”
- Feature 218, “5ESS Switch 5E12 Generic Feature Support”
- Feature 239, “DMS 500 Switch Support”
- Feature 277, “TCP/IP Interface to DMS 100/200 Switches”
- Feature 282, “TCP/IP Interface to 5ESS 5E15 Generic switches”
- Feature 293, “TCP/IP Interface to DMS 250 Switches”
- Feature 296, “TCP/IP Interface to DMS 500 Switches”
- Feature 311, “Enhanced Switch Support for 5ESS Generic 5e15”
- Feature 314, “Enhanced Switch Support for DMS 250 Generic UCS12”
- Feature 315, “Switch Support for *DMS* 500 Generic NCS10”
- Feature 319, “Enhanced Switch Support for DMS 100/200 Generic NA009 Switches”
- Feature 320, “Enhanced Switch Support for DMS 100/200 Generic NA012”
- Feature 321, “Enhanced Switch Support for DMS 500 Generic NCS12”
- Feature 354, “Switch Support for Succession Network Switch Generic SN02”

Other

Surveillance Transition to Trunk Groups greater than 250 (DMS) or 500 (5ESS) requires the following:

- The DCC must be either a FEP (Front End Processor) (NTM) or TDMS (Traffic Data Management System)
- The *DMS* switch must be on generic NA009, UCS12, NCS10 or later
- The *5ESS* switch must be equipped with an Administrative Module (ASM) and a TCP/IP network connects the ASM to the NTM.

□

Setting up DMS 1024 trunk group surveillance — DCC

Purpose

This procedure establishes the link between the host and the FEP.

Before you begin

If the DCC is a TDMS, refer to the TDMS documentation for procedures on creating a link to an NTM host and creating an office to support 1024 trunk groups from a *DMS* switch and skip to Step 3.

Reference: "Building the database for 1024 trunk groups" (p. 22) in the *Record Base Administration Guide*

Instructions

Follow these steps to set up DMS 1025 trunk group surveillance for a DCC:

1 Establish the link on the FEP machine:

a. Create the link (`cnlink`).

b. Activate the link (`anlink`).

c. Activate the link (`aentity`).

Important! This step is only necessary if the link does not already exist.

2 Create the *DMS* switch on the FEP, being sure to specify switch generic NA007 or later (`centity`).

3 Activate (`aentity`).

4 Create the link on the NTM host machine:

a. Add an entry for the DCC in the RSPTE File.

b. For the *DMS* switch entry in the RSPTE File, specify a value for the 'max_tg' entry.

c. Create the RSPTE File (`create rspte`).

d. Enter `stopsys`.

e. Install the RSPTE File (`installdb rspte`).

f. Enter `startsys`.

g. Add an office file for the DCC to indicate the dialstrings for the link.

h. Create the DCC office (`create office`).

i. Activate the DCC office (`act`).

j. Deactivate the *DMS* office if it is activated (`deact`).

k. Create the *DMS* office (`create office`).

l. Activate the office (`act`).

m. `audit <DMS_clli> all`

n. Verify data collection from the *DMS* office.

5 Contact switch personnel to activate their features that correspond to Feature 194 or Feature 238 on the *DMS* switch itself.

6 Activate the *DMS* switch on the DCC.

END OF STEPS

□

Setting up the database for Feature 264

Purpose

This procedure is used to set up the database for Feature 264, "DMS 100/200 Switch Surveillance of 1024 Trunk Groups Via TDM". Use of this feature requires that the System Administrator has set up the links to the TDM and that the Alcatel-Lucent site manager has enabled the appropriate features.

Reference: "Setting up DMS 1024 trunk group surveillance — DCC" (p. 5)

Instructions

Follow these steps to set up the database for Feature 264:

1. Turn on feature ntm-264 (Feature 264, "*DMS* 100/200 Switch Surveillance of 1024 Trunk Groups Via TDM").

2. (Optional) Turn on feature ntm-245 (Feature 245, "TCP/IP Interface to TDM").

3. Add variable `max_tg=1024` to the switch entry in the RSPTE file.

4. Update switch generic to at least `na007` in the RSPTE file.

5. Update TDMS generic for associated TDM in RSPTE file to `tdms3.` (If *DMS* ***does not*** have surveillance of 1024 trunk groups, the TDMS generic should be set to `tdms2`).

6. Turn on 2 locking features:
   - BIGDMS
   - BGDMS100_TDMS

7. (Optional) Turn on the additional locking feature:

- TCPIPTDMS

END OF STEPS

□

Setting up surveillance for more than 250/500 TGs (TCP)

Purpose

This procedure establishes a TCP link between the host and the switch supporting the collection of 1024/2000 trunk groups of data.

Instructions

Follow these steps to set up surveillance for more than 250/500 trunk groups (TCP) by creating a link on the NTM host machine:

1 Add/modify the entry for the DMS switch in the RSPTE File.

2 Specify ‘1024’ for DMS or ‘2000’ for 5ESS for the ‘max_tg’ entry and ‘tcp’ for the ‘direct’ entry.

3 Create the RSPTE file (`create rspte`).

4 Enter `stopsys`.

5 Install the RSPTE file (`installdb rspte`).

6 Enter `startsys`.

7 Add the switch name and IP address in the /etc/hosts file.

8 Add/modify the office file for the switch specifying the required TCP host names and socket numbers.

9 Add additional trunk groups to the trunk group file for this office, specifying options=sched for up to 1024/2000 trunk groups.

10 Deactivate the office if it is activated (`deact`).

11 Create the office (`create office`).

12 Activate the office (`act`).

13 `audit <DMS_clli> all`

14 Verify data collection from the office.

END OF STEPS

□

Troubleshooting

Overview

In the event that all NTM data for a switch being sent through a TDMS/FEP is missing at NTM, you will need to contact TDMS/NTM Customer Support for assistance.

The switch can receive polls using either the EADAS interface (supporting up to 250 TGs) or the newer NTM interface (supporting up to 1024/2000 TGs.)

One possible scenario is that NTM and the switch are set up for 1024 TG support, but TDMS/FEP is not. In this case, TDMS/FEP will send polls for all NTM data for a given switch along the EADAS interface, while the switch expects NTM polls only along the NTM interface.

Such a condition will result in no NTM data for this switch being sent to NTM. In this case, TDMS/FEP should be reconfigured to send NTM polls along the NTM interface.

□

16 UDDM/UDNEI Administration

Overview

Purpose

Previous to release 16 of NTM, support for new data types and support for new network element types has largely been a “coding” exercise in the product carried out by the development team. This model of adding new support basically implied that for any new network element type or any new data type from a new or existing network element type, a customer would have to submit a request to the development team and wait for the next product release. In release 16 of NTM, several features and capabilities have been added to the product that makes it easy for end-users to add such support to the NTM product themselves. This set of features might be referred to as “User-Defined” features. For example, new data types can be defined and added to the system dynamically. This capability is known as User-Defined Data Modeling, or UDDM. It allows for the definition of new periodic, reference, and threshold rule tables to support the new data type. Support for new network element types can also be defined on a deployed system. This capability is known as User-Defined Network Element Interface, or UDNEI.

This capability may require that the end-user creating the support have some amount of programming capability, depending on the complexity of the support. NTM release 16 also provides a capability to transform the data collected via UDNEI to the data model specified using UDDM. This transformation capability performs such functions as field selection and mapping from the data produced by UDNEI, calculations, and threshold testing. Last, but not least, NTM release 16 provides a feature that allows an end-user the ability to construct an analysis on the data collected from the network. This feature is called Enhanced Analysis and Thresholding (of course, we wish we had called it User-Defined Analysis, or UDA). Usually, this involves some combining of the data collected from the network into some new data type. Hence, Enhanced Analysis and Thresholding has a dependency on UDDM. This feature does require some programming skills of the end-user.

These User-Defined features are quite powerful and maybe a little daunting at first glance. To help the user learn to utilize these capabilities, the documentation has been designed from a top down approach. The steps for utilizing these features have been broken down into a set of procedures. These procedures are the main topic of this chapter of the System Administration Guide. These procedures may consist of running some simple Linux commands (e.g. cp or vi) to prepare the user input, running specific commands documented in the *Input Commands Guide* to “load” this input into the system, and possibly running other simple Linux commands to verify the result. The commands referenced in any of these procedures may be new to release 16 of NTM (e.g. `manage_uddm`) or they may be commands that the end-user is already familiar with such as `create` or `thresh`.

Procedures

While the remainder of this chapter documents specific procedures, the rest of this introduction will describe a typical ordering of the procedures for two cases. The first case involves supporting a new network element type that will produce one or more new data types. The second case describes the procedures needed for defining a new analysis. Of course, as the end user becomes more expert in utilizing these user-defined features, these procedures can be utilized in other orders.

In the case that the end user desires to support a new network element type and a new data type, the prescribed procedures are listed in their respective order with brief description of each procedure. Here is the list:

1. Creating a UDDMType – A new periodic data type is created by copying the *template_dat* file, providing the data type specific schema, and loading that schema. At the same time, a reference table and/or a threshold rules table can be created in the exact same manner.
2. Using an existing UDNEI Data Collector – The end user must select a UDNEIType string that declares the intention to utilize a specific data collector in order to support the new network element type. Any given data collector may require its own procedure. For release 16 of NTM, the end user must follow the steps in either Using the simpleftp Data Collector or Using the normalizer Data Collector. The only step in Using the simpleftp Data Collector is optional. There are required steps in Using the normalizer Data Collector.

3. Setting up CC rules – The end-user populates a system provided template file to specify the transformation rules to map collected data to the periodic table specified in Creating a UDDMType. At this point in time, the actual data collector can be started even though no network element instances have been provisioned.
4. Provisioning a network element instance – In this procedure, the end user populates the NTM RSPTE file and provides data collection specific parameter values for the network element instance. Reference data (if such a table was constructed) can be provided at this point or at any time in the future. The end user also will activate data collection for this particular element at the end of this procedure
5. Managing Reference and Thresholds – This procedure can be performed after all preceding procedures have been completed. This procedure is optional and can be repeated as many times as needed. The system will still collect and process data, even if no reference or threshold information has been provided. Of course, as that data is provided, the processing is altered to conform to the input provided.
6. Managing Standalone Reference Tables – This procedure allows you to load reference data into standalone reference tables, which are used for switch-independent reference data lookups. This procedure can be performed after all the preceding procedures have been completed. This procedure is optional and can be repeated as many times as needed.
7. Managing Audits and Managing Controls - These procedures allow you to set up a User Defined audits and controls for UDNE switches.
8. Managing Periodic Data Aggregation and Managing Statistical Thresholding - These procedures allow you to set up a periodic data aggregation and statistical thresholding.

To construct a new analysis, the set of procedures is:

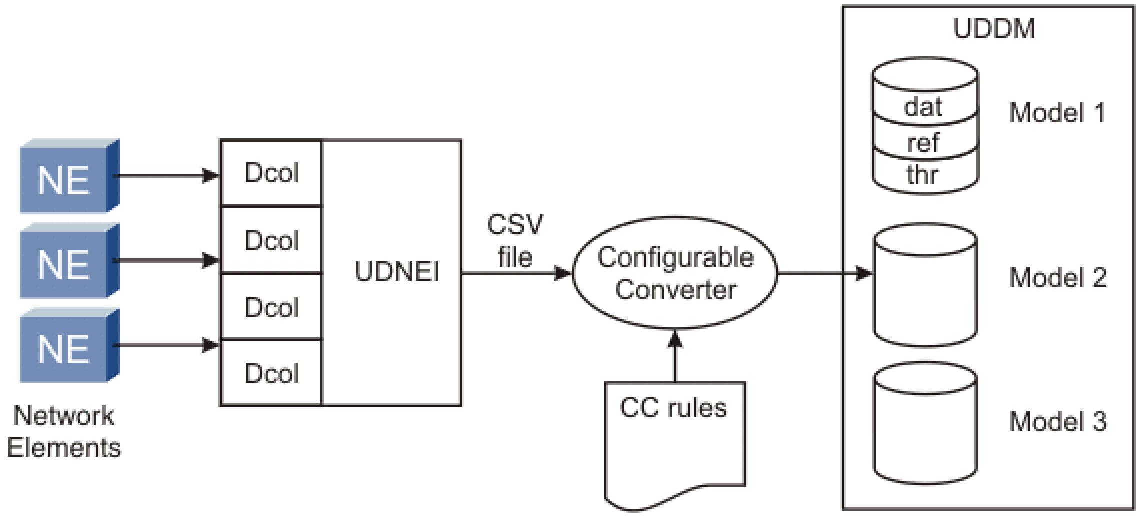
1. Creating a UDDMType – This procedure is previously described.
2. Setting job - With this procedure you can initialize an analysis jobs on the data collected from the network. The parameters and description of configuration files is provided in section How to initialize job.
3. Setting up CC rules - This procedure is previously described.

These two scenarios presents every UDDM/UDNEI creation procedure. Some procedures have corresponding modification and deleting procedures. Those procedures that are very simple may have the mod/delete description embedded in the single procedure. Modifying or deleting a UDDMType is complex enough to warrant its own procedure Modifying/Removing UDDMType.

Overview Diagram

Figure 1 shows an overview of relations between UDDM, UDNEI, and Configurable Converter.

Figure 1 UDDM/UDNEI overview.



BDR Issue

In cases where you utilize the Backup and Disaster Recovery (BDR) feature between a pair of NTM hosts, all user-defined tasks must be manually applied to the second machine. Record base data will be replicated automatically.

Requirements

To perform all the task in this chapter Feature 436, “UDDM/UDNEI” and Feature 437, “Enhanced Thresholding and Analysis” must be purchased. Those features are available since NTM release 16.0 and require the Feature 400, "System Hardware HP Platform and Performance Upgrade".

Important! You must be logged as `nmadm` or some other user in the snm group to run the UDDM/UDNEI commands (See: NMADM login accountability).

Contents

This chapter contains the following topics:

□

UDDM/UDNEI Feature

Overview

Purpose

The Feature 436, “UDDM/UDNEI” include:

- a User Defined Data Modeling (UDDM) capability,
- thresholding of data types defined via UDDM,
- User Defined Network Element Interfaces (UDNEI), and
- transformation capability to map data collected via UDNEI to the data model established via UDDM.

Functionality

With UDDM capability, you can extend the NTM database. This tool allows you to add a specification of new data types for periodic data, for reference data, or for threshold data. When the specification is loaded into the system, physical tables are created to house the data. If a new periodic data type is defined along with companion reference and threshold tables, processing engine in NTM allows the specification of threshold processing rules equal to those provided by Feature 189, “Replacement Thresholding Capability for Trunk Group Data”.

With UDNEI capability, you can add data collection software or use one of the included data collectors to collect data from a newly defined data model. This tool allows you to map fields, perform calculations and thresholding, and perform reference data lookups.

Commands

The following commands have been added to the NTM software for managing the UDDM/UDNEI feature:

- `encrypt_param` - This command encrypts specific parameter in the instance switch file.
- `install_dcol` - Use this command to install UDNEI data collector.
- `manage_ccrules` - Use this command to populate CC configuration tables.
- `manage_dcol_params` - Use this command to manage data collectors parameter files.
- `manage_instance_params` - Use this command to manage Network Element instance parameter files.
- `manage_ssh` - Use this command to manage Network Element instance ssh keys.

- `manage_uddm` - Use this command to manage UDDM data types.
- `manage_udneitype` - Use this command to manage UDNEIType files.
- `udnei_act` - Use this command to start all data collectors for specific UDNEIType.
- `udnei_deact` - Use this command to stop all data collectors for specific UDNEIType.
- `manage_aggr` - Use this command to configure Periodic Data Aggregation.
- `manage_stat` - Use this command to Statistical Thresholding.

  Reference: For more information, see "UDDM/UDNEI Commands" (p. 1) in the *Input Commands Guide*.

GUI Pages

The Periodic Data Browser and Alerts table show the new UDDM data types and statuses for the new UDNEI network elements.

Contents

This chapter contains the following topics:

□

Creating a UDDMType

Purpose

Using this procedure you can extend the NTM database by adding a new User Defined data type (UDDMType).

Template files

The template files: *template_dat, template_ref, and template_thr* reside under the *"/musr/uddm/tables"* directory. Use these template files to create new files for defining the meta data for a new datatype. Each template file supports a comma separated value (CSV) format where you can enter the appropriate values for the new datatype. The periodic data schema file (*<UDDMType>_dat*) is required. The threshold (*<UDDMType>_thr*) and reference (*<UDDMType>_ref*) files are optional. Comment lines started with "#" in the template files are mandatory and they are important for further file processing.

Instructions

Follow these steps to add a new UDDMType.

1 Edit the template files: *template_dat, template_ref, and template_thr* from the */musr/uddm/tables* directory and save as *<UDDMType>_dat, <UDDMType>_ref, <UDDMType>_thr* respectively.

Important! Do not remove the template files. You can use them for the next <UDDMType> definitions.

Reference: See all the available parameters and definitions for *<UDDMType>_dat, <UDDMType>_ref, <UDDMType>_thr files* in manage_uddm section: "Template Files" (p. 33) in *Input Commands Guide*.

2 Execute the `manage_uddm add <UDDMType>` command.

Result: The <UDDMType> tables are added in the Oracle Database. If the need for a reference table was specified, the "*/musr/rb/uddm/<UDDMType>_ref.template*" file is created. That file will be used to input reference records in a future procedure. It was created at this time since the reference schema has just been defined. The *"/musr/uddm/ccrules/<UDDMType>_cc.template*" template file for the Configurable Converter is created. This file will be populated in a future procedure. It was created at this time based on the definition of the periodic table.

3 Optionally if <UDDMType>_ref and <UDDMType>_thr tables are defined for each <UDDMType> a set of threshold files (up to 8) can be created.

Reference: See procedure: "Managing Reference and Thresholds" (p. 18)

END OF STEPS

□

Modifying/Removing UDDMType

Instructions

Follow this steps to modify or remove <UDDMType>.

1 Execute `manage_stat del <UDDMType>` to remove statistical thresholding object using a <UDDMType> you want to remove/modify.

2 Execute `manage_aggr del <UDDMType>` to stop data aggregation using a <UDDMType> you want to remove/modify.

3 Execute `manage_ccrules del <UDDMType>` to stop all CC instances using a <UDDMType> you want to remove/modify.

4 If you want to modify <UDDMType> edit: *"/musr/uddm/tables/<UDDMType>_dat*", "*/musr/uddm/tables/<UDDMType>_ref*", "*/musr/uddm/tables/<UDDMType>_thr*" files.

> **Reference:** See all the available parameters for *<UDDMType>_dat, <UDDMType>_ref, <UDDMType>_thr files* in section "Template Files" (p. 33) in *Input Commands Guide*.

5 Execute `manage_uddm mod <UDDMType>` for modifying or `manage_uddm del <UDDMType>` for removing <UDDMType>.

6 Execute `manage_ccrules add` for all of the <UDDMType>/<UDNEIType(s)>.

END OF STEPS

□

Using an existing UDNEI Data Collector

Purpose

After creating <UDDMType> to collect the data an associated data collector <UDNEI> and related <UDNEIType> must be defined. All the new data collectors will be placed in the *"/nm/udbin"* folder. For each data collector added to the *"/nm/udbin"* a corresponding folder exists in the *"/musr/rb/udnei"*, named the same as the data collector executable program (*"/musr/rb/udnei/<dcol>"*). Parameter files for each network element instance reside under the *"/musr/rb/udnei/<dcol>/<UDNEIType>"* directory.

Instruction

Follow these steps to use a UDNEI data collector:

1 Select a string, less than 30 characters, that we call the UDNEIType string to represent the utilization of the selected data collector for the network element type in mind.

2 Edit the *"/musr/rb/udnei/udneitype"* file and add correct relations between <dcol> and <UDNEIType>.

Example: If the simpleftp data collector were to be used to collect files from the 5ESS and we have select a UDNEIType string of "5ESSFile", a line in this *"/musr/rb/udnei/simpleftp/udneitype"* file would be:

```
udneitype=5ESSFile, dcol=simpleftp
```

3 Perform procedures necessary in utilizing the selected data collector. For the 4 data collectors delivered with the system:

a. simpleftp – See the procedure "Utilizing SimpleFTP Data Collector" (p. 29) for using this collector. There is a properties file for this collector that contains default values for a set of properties. These properties apply to ALL <UDNEITypes> using this data collector. The properties can be edited if needed; however, the default values should be adequate in most cases.

b. normalizer - See the procedure "Utilizing Normalizer Data Collector" (p. 32) for using this collector. There is a properties file for this collector that contains default values for a set of properties. These properties apply to ALL <UDNEITypes> using this data collector. The properties can be edited if needed. In addition, the procedure will describe a programming step that must be completed to provide "map.tcl" and "parse.tcl" scripts that the user must supply. The "map.tcl" script should produce the set of commands necessary to collect the data from the particular network element type in question. The “parse.tcl” script will parse the returned data.

c. SNMP - See the procedure “Utilizing SNMP Data Collector” (p. 49) for using this collector. There is a properties file for this collector that contains default values for a set of properties. These properties apply to ALL <UDNEITypes> using this data collector. The properties can be edited if needed. In addition, the procedure will describe Input and Output DataSet configuration files.

d. SOAP - See the procedure “Utilizing SOAP Data Collector” (p. 55) for using this collector. There is a properties file for this collector that contains default values for a set of properties. These properties apply to ALL <UDNEITypes> using this data collector. The properties can be edited if needed. In addition, the procedure will describe configuration, request, error, and response files.

4 Execute `manage_udneitype add <UDNEItype>` command.

Result: The combination of <UDNEIType> and <dcol> is inserted into the Oracle Database. The command creates *"/musr/rb/udnei/<dcol>/<UDNEIType>"* and *"/musr/swdata/udnei/<UDNEIType>"* folders. The *“/musr/rb/udnei/<dcol>/<UDNEIType>”* folder will be used to create network element instance files for parameters particular to the <dcol> and values particular to the network element instance. The *“/musr/swdata/udnei/<UDNEIType>”* folder will be used for temporary data files.

5 To run the <dcol> execute `udnei_act <UDNEIType>` command.

Important! No network element instances are provisioned at this point in time. This activation could wait until the first network element is provisioned.

Important! In order to allow more than 10 (default value) direct connections to UD items, you must change the value of `per_source` parameter in the */etc/xinetd.conf* configuration file.

END OF STEPS

□

Modifying/Removing UDNEI Data Collector

Instructions

Follow this steps to modify or remove <UDNEIType> data collector.

1 Edit *"/musr/rb/rspte/rspte"* and remove all Network Elements using <UDNEIType> which will be removed or modified.

2 Execute `create all` command.

3 Execute `installdb all` command.

4 If you want to modify <UDNEIType> edit *"/musr/rb/udnei/udneitype"* file.

5 Execute `manage_udneitype mod <UDNEItype>` for modifying <UDNEIType> or `manage_udneitype del <UDNEItype>` for removing <UDNEIType>.

END OF STEPS

□

Setting up CC rules

Purpose

After creating specific <UDDMType> and <UDNEI> network element raw data from Data Collection network element must be populated into the Oracle database. The Configurable Converter (CC) is a subsystem which populates this data provided by Data Collection network elements into the Oracle database. The CC is responsible for the following tasks:

- getting raw data from DCOL,
- executing all user-defined calculations,
- applying threshold rules,
- performing lookups of reference data.

For each triple: <UDDMType> and related <UDNEI> and <dcol>, one CC instance must be configured. To configure the CC instance use the `manage_ccrules` command.

CC Template File

The `manage_uddm` command creates a template file for the `manage_ccrules` command. You must add CC rules for each field in this file in specific order. First is the rule for period field. Then rules for key and attribute. Next are the raw data followed by the calc fields. If you are doing an analysis job define them after comment line "#apply threshold tests". The Configurable Converter applies threshold tests just after performing user defined calculations.

Reference: See the list of primitives for creating CC rules "Primitives" (p. 17) in the *Input Commands Guide*.

Instructions

Follow these steps to configure a CC instance:

1 Edit *<UDDMType>_cc.template* file. Add the number of fields that make up input records in the CSV file (`numfield` parameter). Also, add CC rules for each field listed in this file. If this file is being prepared to consume data from a udnei data collector, rename this rule file to *<UDDMType>_<UDNEIType>_cc*. If the rule file is to process data from an analysis job, rename the file to *<UDDMType>_cc*.

Reference: The file *<UDDMType>_cc.template* is created in the procedure "Creating a UDDMType" (p. 8).

2 Execute `manage_ccrules add <UDDMType> [<UDNEIType>] [<dcol list>] [<suffix>]`.

Result: The CC rules from the *<UDDMType>_cc.template* file are inserted into the Oracle Database. This command creates *"/musr/hod/<UDNEIType>/<UDDMType>[_suffix]"* directory.

3 Optional: Check if CC instance is running with -s <sourcename> option.

Important! Each combination of <UDDMType>_<UDNEIType>_<suffix> is called internally as sourcename.

END OF STEPS

□

Provisioning a network element instance

Before you begin

Before utilizing this procedure “Provisioning a network element instance” create the <UDDMType(s)>, specify the <UDNEIType> and associated data collectors and define the appropriate CC rules.

References: See “Creating a UDDMType” (p. 8), “Using an existing UDNEI Data Collector” (p. 11), and “Setting up CC rules” (p. 14).

Instruction

Follow these steps to maintain a network element instance:

1. Edit RSPTE to add a row labeling it with the <UDNEIType> string in the last field called udneitype.

   Example: The line in the *“/musr/rb/rspte/rspte”* file looks similar to the following:

   ```
   ohudne_30, 123123123133030,,,,udne,udne1,1,,n,,ohudnei;
   ```

2. Execute `dbtest rspte`

3. Execute `create rspte`

4. Stop the system executing `stopsys`

5. Execute `installdb rspte now`

6. Start the system executing `startsys`

7. Edit the file *“/musr/rb/udnei/<dcol>/<UDNEIType>/<clliname>”* to supply parameter values for this network element instance.

   Reference: See available parameters in the “Template File” (p. 8-26) definition of `manage_instance_params` command.

8 If it desirable to encrypt any of the parameter values for this network element, execute `encrypt_param <clliname> <parameter name> <parameter value>`

Result: The following <parameter value> of the <parameter name> in the <clliname> file is encrypted.

Important! *"/musr/rb/udnei/<dcol>/<UDNEIType>/<clliname>"* file is required to create office that has udneitype defined in rspte.

9 In the */musr/rb/uddm* directory, edit the *<UDDMType>_ref.template* file and save as *<UDDMType>_<clliname>* in the same directory.

Important! This step is optional. Even if a reference file was created during `manage_uddm`, the absence of this file will only trigger a warning. The file may be present, but empty as well. After the office is provisioned and even collecting data, this file can be edited and the office re-created.

10 Execute `dbtest office <clliname>`

11 Execute the `create office <clliname>` command.

Result: The file *<UDDMType>_<clliname>* is populated in the Oracle Database.

12 If needed execute `udnei_act <UDNEIType>`

13 Execute `act <clliname>` command.

14 If this is a regular office run `office audits`

15 If you need to change the parameters you can execute `manage_instance_params mod <clliname>` command. This command is executed by `create office` command in Step 11 of this procedure.

END OF STEPS

□

Managing Reference and Thresholds

Purpose

This procedure can be performed after all preceding procedures from this chapter have been completed. This procedure is optional and can be repeated as many times as needed. If you want to set up thresholding the threshold (*<UDDMType>_thr*) and reference (*<UDDMType>_ref*) files must be defined. Similar to the procedure "Scheduling threshold tables" (p. 3-23) you can set up a schedule for thresholding using <uddm_table>.

Instructions

Follow these steps to define thresholding:

1 For each <UDDMType> a set of threshold files (up to 8) can be created. Save them as <UDDMType>_thresh<#> files in the *"/musr/rb/thresh"* directory.

> **Reference:** See more information about Thresholds in Chapter 5, "Thresholds" in the *System Overview*.

2 Load the threshold files using `thresh <UDDMType>_thresh<#>` command.

> **Result:** Each threshold file is named according to the following format: *<UDDMType>_thresh<#>* and is located under the *"/musr/rb/thresh"* directory.

3 For defined threshold files you can define schedule for thresholding by editing *"/musr/rb/thresh/sched"* file and adding <uddm_table>:

> **Example:** This is an example from *"/musr/rb/thresh/sched"* file.

```
day=sunday,
start=00:00,tg_table=1;
start=08:00,tg_table=1;
start=17:00,tg_table=1;
start=22:00,tg_table=1;

start=00:00,demo_table=1;
start=11:00,demo_table=3;
start=12:00,demo_table=2;
start=13:00,demo_table=4;
```

Reference: See “Scheduling threshold tables” (p. 3-23)

□

Managing Standalone Reference Tables

Before you begin

Before utilizing this procedure "Managing Standalone Reference Tables," create the <UDDMType(s)>, specify the <UDNEIType> and associated data collectors, and define the appropriate CC rules.

> **References:** See "Creating a UDDMType" (p. 8), "Using an existing UDNEI Data Collector" (p. 11), and "Setting up CC rules" (p. 14).

Instruction

Follow these steps to maintain a network element instance:

---

1 Edit the template file *template_ref* from the */musr/uddm/tables* directory and save it as *<RefDataType>_ref*. Replace *<RefDataType>* with a name that represents the type of reference data. In this file, define the reference data table structure.

---

2 Execute this command to create the table:

```
manage_uddm add <RefDataType>
```

> **Result:** This command creates an input template file named *<RefDataType>.template* in the */musr/rb/ref* directory.

---

3 Edit the template file *<RefDataType>.template* in the */musr/rb/ref* directory and save it as *<RefDataType>* (with no file extension). Add the reference data records you want to load in the file, one record per line.

Add each record in the format:

```
<field1>=<value>,<field2>=<value>,...<fieldN>=<value>;
```

Each record should contain the name of each field in the reference table, followed by a value for the field. Separate field/value pairs with commas, and end each record with a semicolon.

---

4 Execute this command to test the validity of the data file:

```
dbtest ref <RefDataType>
```

If `dbtest` returns errors, edit the *<RefDataType>* file to correct the errors, then run the `dbtest` command again until no errors are found.

5 Execute this command to load the data file:

```
create ref <RefDataType>
```

Important! If there is already data in the reference table when you run this command, the existing data will be completely erased, and then the data in the file will be loaded. If you are making an update to the reference data, make sure the *<RefDataType>* file contains ***all*** the reference data, not just new or changed records.

END OF STEPS

Managing Audits

Purpose

Using this procedure you can add the audit to the NTM. For modifying or removing audits use the appropriate mod/del actions of the `manage_audit` command.

Instructions

Follow these steps to define audits:

1. Create */musr/uddm/audits/<audit_name>_audit* file. You can use the template_audit file as the base.

   Reference: See all the available parameters for *<audit_name>_audit* file in the section "Template File" (p. 8) in *Input Commands Guide*.

2. Execute `manage_audit add <audit_name>`

3. Edit */musr/uddm/audits/assignments/audit_assignments* file and add audit name with assignment to dcols.

   Example: The is an example of the *musr/uddm/audits/assignments/audit_assignments* file.

   ```
   eplist,nextonersm,soap;
   rlmlist,nextonersm,soap;
   ```

4. Execute `manage_audit assign <audit_name>`

END OF STEPS

□

Managing Controls

Purpose

Using this procedure you can add the controls to the NTM. For modifying or removing controls use the appropriate mod/del actions of the `manage_control` command.

Instructions

Follow these steps to define controls:

1 Edit the *template_ctl* file and save as *<UDDMType>_ctl*

Reference: See all the available parameters for *<UDDMType>_ctl* file in the section "Template Files" (p. 33) in *Input Commands Guide*.

2 Execute `manage_uddm add <UDDMType>`

Result: The */musr/uddm/controls/<UDDMType>_control.template* file is created.

3 Edit the */musr/uddm/controls/<UDDMType>_control.template* file and save as */musr/uddm/controls/<control_name>_control* file.

Reference: See all the available parameters for *<control_name>_control* file in the section "Template File" (p. 10) in *Input Commands Guide*.

4 Execute `manage_control add <control_name>`

5 Edit */musr/uddm/controls/assignments/control_assignments* file and add control name with assignment to dcols.

Example: The is an example of the *musr/uddm/controls/assignments/control_assignments* file.

```
ratelimit,nextonersm,soap;
```

6 Execute `manage_control assign <control_name>`

END OF STEPS

□

Managing Periodic Data Aggregation

Purpose

Using this procedure you can aggregate periodic data at hourly, daily, or monthly levels.

Properties

Default configuration parameters for the periodic data aggregation engine are provided in the */nm/rdb/config/aggregation.conf* file. Parameters in this file are arranged in the list of key-value pairs. Changing initial values will not affect already created aggregations, only the new ones. The default file contains the following information:

- Tablespace where aggregation tables will be created.
- Default offset in minutes. Offset determines start of the job after an end of the aggregation period.
- Definition of how many times retention is longer than for a _DAT table.
- Default formula for number type columns.

Instructions

Follow these steps to define aggregations:

1 Execute `manage_aggr initfile <UDDMType>`

Result: The */musr/uddm/tables/<uddm type>_aggr* configuration file will be created.

Hint: The created file will contain default values pre-populated, such as: source table name, aggregation level, list of non-key columns names with default formulas for NUMBER columns.

2 Edit the configuration by executing `manage_aggr edit <UDDMType>`

Hint: This command uses the EDITOR environment variable to determine a text editor. If this variable is not set, `vim` *is assumed.*

3 When finished editing the configuration file run `manage_aggr add <UDDMType>`

Result: Aggregation will be created and status will be displayed.

Important! In order to delete data aggregation for particular data type you need to delete at first the statistical thresholds for that data type.

END OF STEPS

<UDDMType>_aggr File Example

The <UDDMType>_aggr file contains two types of information. The information included in the first line of the file, describes the following:

- Model - name of the table for UDDMType.
- Aggregation level - the option to specifies the need of periodic data type. The value set for that option is:
  - 'H' hourly aggregation.
  - 'D' value implies both Hourly and Daily aggregations.
  - 'M' value will add Monthly aggregation to the previous 2 levels.
- Offset - value must fall in the range [2-168] and signifies the need to compute statistical thresholds.
- Occurrences - number of occurrences, must fall in the range [1-6] if offset is set.

Every next line presents aggregation formulas:

- Field name - non key UD field name specified for UDDMType.
- Formula - Oracle expression used for the aggregation of the specified field name. If the formula contains a comma separator, then the whole expression must be enclosed in double quotes.
- Is thresholdable - 'y' indicates that for this field the statistical thresholding is active.

This is an example of populated sbc_aggr file:

```
# source table name (<type>_dat), aggregation level (H,D,M), offset,
occurrences
SBC_DAT,H,2,1;
# column name, formula, statistical thresholding enabled (y/n)
MAXSDRLAGTIME,SUM(MAXSDRLAGTIME),;
SDRS,AVG(SDRS),y;
```

Explanation of the all lines in the example:

1. The aggregation will be computed for `SBC_DAT` table, with the hourly period. Next values (2,1) implies that the means will be computed from data that is from 2 hours ago. For example, if we are computing the statistical thresholding mean for current data at 11:05, we should be looking at the data for the 9:00 hour (9:00 through 9:55).
2. The `SUM` Oracle formula will be used for aggregation of field `MAXSDRLAGTIME`. This field won't be used in statistical thresholding.
3. The `AVG` Oracle formula will be used for aggregation of field `SDRS`. This field will be used in statistical thresholding.

Managing Statistical Thresholding

Purpose

Statistical thresholding is beneficial in cases where the user is unfamiliar with the performance behavior of the network object want to compare current behavior with history. In order to perform this style of threshold testing, a performance system must track the historical performance of a network object in order to create an historical mean that is then compared to newly reported values. In NTM, such historical averages are computed from data saved by a separate Feature 460, “Periodic Data Aggregation”.

Instructions

Follow these steps to define statistical thresholding for particular data type:

1. Make sure that for a given `<UDDMType>` the periodic data aggregation is started. Add to */musr/uddm/tables/<UDDMType>_aggr* file lines with thresholdable fields. For more information, see Managing Periodic Data Aggregation.

2. Execute `manage_stat add <UDDMType>`

   Result: This command will add proper data type to statistical tresholding engine.

3. For given UDDMType execute `manage_ccrules mod <UDDMType>`

4. Edit and load the threshold files using `thresh <UDDMType>_thresh<#>` command.

   Reference: See Managing Reference and Thresholds.

END OF STEPS

□

Utilizing SimpleFTP Data Collector

Simple FTP Collector

The `simpleftp` data collector provides the possibility to collect the data using ftp connection. The following parameters for a specified network element type and their respective values for network element instances of that type are collected:

- IP - IP number or host name.
- User - ftp user name.
- Passwd - ftp password.
- Periodicity - period for collecting data (allowed values are: 5, 15, 30, or 60 minutes)
- Offset - offset time to start collecting data in milliseconds.
- Filename. The Filename parameter contains the following meta-variables:
  - Letter - Date or Time Component
  - y - Year (00-99)
  - Y - Year (4-digit)
  - m - Month in year (01-12)
  - d - Day in month (01-31)
  - e - Day in week (0-6)(starts from Sunday)
  - E - Day in week (0-6)(starts from Monday)
  - H - Hour in day (00-23)
  - M - Minute in hour (00-59)
  - S - Second in minute (00-59)
  - X - Period in day (001-288)
  - C - Entity id
  - T - Entity type
- Directory - directory with *`Filename`* file.
- Timeout (optionally) - Timeout for FTP connection (in milliseconds).

Then the data is prepared for a Configurable Converter.

Simpleftp_clli File Example

This is an example of populated simpleftp_clli file:

```
paramName=IP,paramValue=meas_host,encrypted=n
paramName=User,paramValue=meas_user,encrypted=n
paramName=Passwd,paramValue=meas_passwd,encrypted=n
paramName=Periodicity,paramValue=5,encrypted=n
```

```
paramName=Offset,paramValue=30,encrypted=n
paramName=Filename,paramValue=%Y-%m-%d_%H:%M,encrypted=n
paramName=Directory,paramValue=/home/measurements,encrypted=n
paramName=Timeout,paramValue=1000,encrypted=n
```

Properties

All the parameters for `simpleftp` must be provided in the *"/musr/rb/udnei/simpleftp/simpleftp.properties"* file. The properties file can be changed during DCOL process. It will be updated in the next 5-min. period. The "*udnei_simpleftp.<#>"* log files reside under the *"/musr/tracer/"* folder. The following is the list of available parameters for *"simpleftp.properties"*:

- kernel.threads - Number of parallel scan threads. The default is 1.
- kernel.retryInterval - Time between two connection/scan attempts for one network element in milliseconds. The default is 10,000 milliseconds. Maximum value is 280,000 milliseconds.
- kernel.logSize - Size of the log file. The default is 1,000,000.
- kernel.logRotate - Number of the log files. The default is 2.
- kernel.jobTimeout - job timeout in milliseconds - the maximum time allowed for a job execution. The default is 5000.
- kernel.logFormat - Format of the log files: TEXT or XML. The default is TEXT.
- kernel.logLevel - The logging level. It is updated every 5 minutes. One of the following option: NONE, SEVERE, WARNING, INFO, FINE, FINER, FINEST, ALL. The default is WARNING.
- kernel.logEntity - name of NE entity that log is filtered for, empty means log is not filtered
- defaultTimeout - default timeout for a single FTP command (in milliseconds).
- kernel.retries - the number of how many times failed job should be retried. The maximum value is 10.

Examples

Each pattern letter is preceded with % sign. The following is an example of filename parameter:

```
“%y%m%d_%H%M%S” 060714_081213
“%C_%e_%X”clli_2_144 (that is 144th period of Monday for clli)
```

Instructions

Follow these steps to utilize a simpleftp data collector:

1 The default properties file should be fine, but you can edit the *"/musr/rb/udnei/simpleftp/simpleftp.properties"* file.

Reference: See the "Properties" (p. 30)

END OF STEPS

Reference

See "Using an existing UDNEI Data Collector" (p. 11), "Modifying/Removing UDNEI Data Collector" (p. 13), and "Provisioning a network element instance" (p. 16) procedures.

□

UDNEI Normalizer

The `normalizer` data collector provides the possibility to collect the following parameters for a specified network element type and their respective values for network element instances of that type provisioned to the user:

- IP - IP number or host name.
- User - ftp user name.
- Passwd - ftp password.
- Periodicity - period for collecting data (allowed values are: 5, 15, 30, or 60 minutes)
- Offset - offset time to start collecting data in milliseconds.
- Timeout - timeout value in milliseconds.

Then the data for each UDDMType is prepared for a Configurable Converter.

Normalizer_clli File Example

This is an example of populated normalizer_clli file:

```
paramName=IP,paramValue=meas_host,encrypted=n
paramName=User,paramValue=meas_user,encrypted=n
paramName=Passwd,paramValue=meas_passwd,encrypted=n
paramName=Periodicity,paramValue=15,encrypted=n
paramName=Offset,paramValue=0,encrypted=n
paramName=Timeout,paramValue=5000,encrypted=n
```

Properties

All the dcol parameters for `normalizer` must be provided in the *"/musr/rb/udnei/normalizer/normalizer.properties"* file. The properties file can be changed during DCOL process. It will be updated in the next 5-min. period. The "*udnei_normalizer.<#>"* log files reside under the *"/musr/tracer/"* folder. The following is the list of available parameters:

- kernel.threads - Number of parallel scan threads. The default is 1.
- kernel.retryInterval - Time between two connection/scan attempts for one network element in milliseconds. The default is 10,000 milliseconds. Maximum value is 280,000 milliseconds.
- kernel.logSize - Size of the log file. The default is 1,000,000.
- kernel.logRotate - Number of the log files. The default is 2.
- kernel.jobTimeout - job timeout in milliseconds - the maximum time allowed for a job execution. The default is 5000.

- kernel.logFormat - Format of the log files: TEXT or XML. The default is TEXT.
- kernel.logLevel - The logging level. One of the following option: NONE, SEVERE, WARNING, INFO, FINE, FINER, FINEST, ALL. The default is WARNING.
- kernel.logEntity - name of NE entity that log is filtered for, empty means log is not filtered
- defaultTimeout - default timeout for a single FTP command (in milliseconds).
- kernel.retries - the number of how many times failed job should be retried. The maximum value is 10.

TCL Files

Normalizer uses two files *map.tcl* and *parse.tcl*. File *map.tcl* is used for creating a sequence of ftp commands for retrieving data. File *parse.tcl* is used for validation and processing of the retrieved data.

In the file *map.tcl*, function periodic() must be created. The following are the parameters for the periodic function:

- input parameters:
  - NeName - Network Element name
  - Function - Network Element function (UDNEI type)
  - CmdSeparator - separates each ftp command. Append this to the TCLOutBuf between each ftp command needed to get/put a file.
  - RmtAddr - remote host name/IP
- output parameters:
  - TCLReturn - OK or MAPERROR
  - TCLOutBuf - message(s) to send to the UDNE (FTP commands)

In the file *parse.tcl*, functions parse1() and periodic() must be created. The following are the parameters for the parse1 function in the *parse.tcl* file:

- input parameters:
  - NeName - Network Element name
  - Function - Network Element function (UDNEI type)
  - ChlType - Periodic=8
- output parameters:
  - TCLReturn - OK or MAPERROR
  - TCLRptType - The raw data report type as "Periodic"

The following are the parameters for the periodic function in the *parse.tcl* file:

- input parameters:
  - NeName - Network Element name

    - Function - Network Element function (UDNEI type)
    - DataFile - Name of the file with data for parsing
- output parameters:
    - out TCLReturn - OK - success; FAIL - Failure parsing periodic response
    - out TCLOutBuf - The list of *attr_values* need not include the Network Element name nor the Period timestamp as the normalizer will prepend these to each record. The buffer containing object data should be in the following format: `<UDMM Type>Periodic:<attr_value>,<attr_value>...`
    - out TCLOutTbl - The periodic table name as it appears in the SupportedTables section of the object configuration file.
    - UDDM_<UDMM type>Periodic

Commands

Here is the set of commands with parameters which you can use in *map.tcl* file:

- `cd <remote directory>`
- `get <remote file> <local directory/file>`
- `mget <remote file pattern> <local directory>`
- `mkdir <remote directory>`
- `rename <from remote directory/file> <to remote directory/file>`
- `rmdir <remote directory>`

Map.tcl Example

This is an example of *map.tcl* file:

```
#  TCL script to map NTM requests to commands to send to a UDNE which
#  supports an telnet interface.

#
#  proc Periodic
#  -------------
#  Create buffer of command(s) to send to UDNE for Periodic data
#  collection. If the command(s) change depending on the function of
#  the UDNE, the global variable Function may be accessed.  This mapping
#  procedure is called once per periodic interval.
#
#  Output:
# TCLOutBuf - Formatted Periodic data collection message(s)
#    to send to the UDNE
# TCLOutSizes - Size in bytes of message(s) separated with white
#    space (\t or <blank>)
# TCLReturn, possible values:
```

```
#      "OK"
#      "MAPERROR"
#
proc Periodic { } {

    global TCLOutBuf
    global TCLReturn
    global TCLOutSizes
    global CmdSeparator

    global NeName
    global RmtAddr
    global Function

    #  Clear the output buffer
    set TCLOutSizes 0
    if [info exists TCLOutBuf] {
        unset TCLOutBuf
    }

    set TCLOutBuf ",,,"
    append TCLOutBuf $CmdSeparator
    append TCLOutBuf "$NeName:,date >> dateList,,"
    append TCLOutBuf $CmdSeparator
    append TCLOutBuf "$NeName:,cat dateList,,"
    append TCLOutBuf $CmdSeparator
    append TCLOutBuf "$NeName:,,write,/tmp/dateList.$NeName.out"

    set TCLOutSizes [string length $TCLOutBuf]
    ntm_trace "TCLOutBuf is " $TCLOutBuf
    ntm_trace "TCLOutSizes is " $TCLOutSizes

    set TCLReturn "OK"
    Debug_Proc "Periodic"

    return
}
```

Parse.tcl Example

This is an example of *parse.tcl* file:

```
#  TCL script for parsing and normalizing data from User Defined NE
#
#  proc Parse1
#  -----------
#  First pass TCL parsing.  Check the message type to see if this is one of
#  the types we're looking for, based on which channel data was collected.

proc Parse1 {} {
```

```
global ChlType

global TCLReturn
global TCLRptName
global TCLRptType
global TCLAudType
global TCLOutBuf

global NeName
global Function

ntm_trace "Parse1 ChlType:" $ChlType

# Initialize TCLRptName, etc
set TCLRptName "None"
set TCLRptType "Unknown"
set TCLOutBuf "\n"
set TCLReturn "OK"

#

if { [ hasPeriodic $ChlType] == 1 } {
         ntm_trace " This must be Periodic Data"
    ###  UDNE  ###

    set TCLRptName "data"
    set TCLRptType "Periodic"
    ntm_trace "Report type:" $TCLRptType " Rpt:" $TCLRptName
    Debug_Parse1
    return
}

if { [ hasMessage $ChlType] == 1 } {

    ###  UDNE  ###

    #  Add specific code to recognize Message report(s).

   set TCLRptName "<UDNE RawString2>"
   set TCLRptType "Message"
   ntm_trace "Report type:" $TCLRptType " Rpt:" $TCLRptName
   Debug_Parse1
   return
}

if { [ hasAudit $ChlType ] == 1 } {

    ###  UDNE  ###
```

```
       #  Add specific code to recognize Audit report(s).

     set TCLRptName "<UDNE RawString3>"
     set TCLRptType "Audit"

#    if { audit is reference audit } {
#        set TCLAudType "RefAudit"
#    }

#    if { audit is control audit } {
#        set TCLAudType "CtlAudit"
#    }

     ntm_trace "Report type:" $TCLRptType " Rpt:" $TCLRptName " Audit Type"
   $TCLAudType
     Debug_Parse1
     return
   }

   if { [ hasControl $ChlType ] == 1 } {

       ###  UDNE  ###

       #  Add specific code to recognize Control report(s).

     set TCLRptName "<UDNE RawString4>"
     set TCLRptType "Control"
     ntm_trace "Report type:" $TCLRptType " Rpt:" $TCLRptName
     Debug_Parse1
     return
   }

   if { [ hasPkgSchedule $ChlType ] == 1 } {

       ###  UDNE  ###

       #  Add specific code to recognize Package Schedule
       #  report(s).
       #  NOTE:  PkgSchedule responses are not used to update
       #  the rawDataStatus object (TCLRptName = "None").

     set TCLRptName "None"
     set TCLRptType "Schedule"
     ntm_trace "Report type:" $TCLRptType " Rpt:" $TCLRptName
     Debug_Parse1
     return
   }
}
```

```
#
#  proc Periodic
#  -------------
#  Parse and normalize Periodic report data.  Return value indicates
#  whether or not the report is parsed successfully.
#

proc Periodic {} {

   global TCLRptName
   global array PerLimit

   global TCLReturn
   global TCLOutBuf
   global TCLOutTbl

   global NeName
   global Function

   ntm_trace "Parse Periodic RptName:" $TCLRptName

   set TCLReturn "FAIL"
   set TCLOutBuf "\n"
   set TCLOutTbl "None"

   ###  UDNE  ###

   switch -regexp $TCLRptName \
       "data" { Perdata } \
       default { ntm_trace "Unknown Periodic rptName: " $TCLRptName }

   #  End buffer with newline.  Safer this way.
   append TCLOutBuf "\n"

   Debug_Proc "Periodic"
   return
}

#
#  ###  UDNE  ###
#
#  proc Perdata<raw1>

proc Perdata { } {
   global NeName
   global array PerLimit
   global DEBUG
global TCLReturn
global TCLOutBuf
global TCLOutTbl
global Function

set FUNCTN [string toupper $Function]
ntm_trace $Function $FUNCTN

ntm_trace "In Perdata"
set TCLOutBuf "\n"
set Dir "/tmp"
set F0 [ string toupper $NeName ]
set F1  "$F0.FIVE.CSV"

      if [ catch { set list [exec ls -tr $Dir/$F1 ] } err ] {
   ntm_trace "Error $err: Most likely the switch did not produce any file"
   return
}
      set num [expr [llength $list] - 1]
      set actList [split $list \n\r]
      set fileName [lindex $actList $num]
ntm_trace "filename is: " $fileName

if [ catch { open $fileName r } input ] {
  ntm_trace "Cannot open input file for reading"
} else {
  foreach line [split [ read $input] \n] {
   if { [ regexp -- ",TRKQOSOM," $line match ] } {
       ntm_trace "Line match TRKQOSOM"
       ntm_trace "$line\n"

            ProcessTRKQOSOM $line

   } elseif { [ regexp -- ",GWCTKQOS," $line match ] } {
       ntm_trace "Line match GWCTKQOS"
       ntm_trace "$line\n"

       ProcessGWCTKQOS $line

   } else {
       ntm_trace "Line no match"
   }
  }
set TCLReturn "OK"
}

#if { ! $DEBUG } {
    #file delete "$fileName"
#}
```

```
   return
}
```

Trace Function

If you want to do a trace function in NTM use `ntm_trace` command .

Example: This is a line from tcl code with `ntm_trace` command:

```
ntm_trace "switch IP " $RmtAddr  $NewStamp
```

Instructions

Follow these steps to utilize a normalizer data collector:

1 The default properties file should be fine, but you can edit the *"/musr/rb/udnei/normalizer/normalizer.properties"* file.

Reference: For the list of parameters, see the "Properties" (p. 32)

2 Edit *"/musr/rb/udnei/normalizer/map.tcl"* and *"/musr/rb/udnei/normalizer/parse.tcl"* files.

Reference: For the list of parameters, see the "TCL Files" (p. 33)

END OF STEPS

Reference

See "Using an existing UDNEI Data Collector" (p. 11), "Modifying/Removing UDNEI Data Collector" (p. 13), and "Provisioning a network element instance" (p. 16) procedures.

□

Utilizing sftp_normalizer Data Collector

Purpose

The sftp_normalizer data collector provides the possibility to collect the following parameters for a specified network element type and their respective values for network element instances of that type provisioned to the user:

- IP - IP number or host name.
- User - ftp user name.
- Passwd - ftp password.
- Periodicity - period for collecting data (allowed values are: 5, 15, 30, or 60 minutes)
- Offset - offset time to start collecting data in milliseconds.
- Timeout - timeout value in milliseconds.

The sftp_normalizer provides the same functionality as normalizer data collector. The only difference is that sftp_normalizer is using secure ftp protocol. For all the available parameters in the *"/musr/rb/udnei/sftp_normalizer/parameters"* and *"/musr/rb/udnei/sftp_normalizer/sftp_normalizer.properties"* see: "Utilizing Normalizer Data Collector" (p. 32). However note that IP parameter must have "sftp://" prefix for secure ftp connection.

Instructions

Follow these steps to utilize a sftp_normalizer data collector:

1 The default properties file should be fine, but you can edit the *"/musr/rb/udnei/sftp_normalizer/sftp_normalizer.properties"* file.

Reference: For the list of parameters, see the "Properties" (p. 32)

2 Edit *"/musr/rb/udnei/sftp_normalizer/map.tcl"* and *"/musr/rb/udnei/sftp_normalizer/parse.tcl"* files.

Reference: For the list of parameters, see the "TCL Files" (p. 33)

END OF STEPS

Reference

See “Utilizing Normalizer Data Collector” (p. 32), “Using an existing UDNEI Data Collector” (p. 11), “Modifying/Removing UDNEI Data Collector” (p. 13), and “Provisioning a network element instance” (p. 16) procedures.

□

Utilizing telnet_normalizer Data Collector

Purpose

The `telnet_normalizer` is a normalizer-like data collector which utilizes a telnet connection. The user has the ability to provide a TCL map and parse scripts. The fetcher in this data collector consumes commands created by the TCL map script and invoke appropriate telnet connection functions.

Telnet_normalizer data collector provides the possibility to collect the following parameters for a specified network element type and their respective values for network element instances of that type provisioned to the user:

- IP - IP number or host name.
- User - user name.
- Passwd - password.
- Prompts - determines the telnet login/password prompts dialect (allowed values are: default or dms500; if empty the `default` is used).
- Periodicity - period for collecting data (allowed values are: 5, 15, 30, or 60 minutes)
- Offset - offset time to start collecting data in milliseconds.
- Timeout - Timeout value in milliseconds.

Telnet_normalizer_clli File Example

This is an example of populated telnet_normalizer_clli file:

```
paramName=IP,paramValue=meas_host,encrypted=n
paramName=User,paramValue=meas_user,encrypted=n
paramName=Passwd,paramValue=meas_passwd,encrypted=n
paramName=Prompts,paramValue=default,encrypted=n
paramName=Periodicity,paramValue=15,encrypted=n
paramName=Offset,paramValue=0,encrypted=n
paramName=Timeout,paramValue=5000,encrypted=n
```

Properties

All the dcol parameters for `telnet_normalizer` must be provided in the *"/musr/rb/udnei/normalizer/telnet_normalizer.properties"* file. The properties file can be changed during DCOL process. It will be updated in the next 5-min. period. The "*udnei_telnet_normalizer.<#>"* log files reside under the *"/musr/tracer/"* folder. The following is the list of available parameters:

- kernel.threads - Number of parallel scan threads. The default is 1.

- kernel.retryInterval - Time between two connection/scan attempts for one network element in milliseconds. The default is 10,000 milliseconds. Maximum value is 280,000 milliseconds.
- kernel.logSize - Size of the log file. The default is 1,000,000.
- kernel.logRotate - Number of the log files. The default is 2.
- kernel.jobTimeout - job timeout in milliseconds - the maximum time allowed for a job execution. The default is 5000.
- kernel.logFormat - Format of the log files: TEXT or XML. The default is TEXT.
- kernel.logLevel - The logging level. One of the following option: NONE, SEVERE, WARNING, INFO, FINE, FINER, FINEST, ALL. The default is WARNING.
- kernel.logEntity - name of NE entity that log is filtered for, empty means log is not filtered
- defaultTimeout - default timeout for a single user command (in milliseconds).
- kernel.retries - the number of how many times failed job should be retried. The maximum value is 10.

TCL Files

Telnet_normalizer uses two files *map.tcl* and *parse.tcl*. File *map.tcl* is used for creating a sequence of commands for retrieving data. File *parse.tcl* is used for validation and processing of the retrieved data.

The syntax of the commands created by the map TCL script consists of multiple command lines of the following format:

`Search string, Input, Action, FileName`

`Search string`text to search for on the STDOUT of the telnet connect.

`Input` next “command” to write on the STDIN of the telnet connection.

`Action` field will be limited to {null|write|append}.

`FileName` local file to which the captured STDOUT data is written (or appended to).

> **Reference:** All the parameters and examples of TCL files you can find in the Normalizer Data Collector section “TCL Files” (p. 16-33).

Example

The following is a set of command example from TCL script:

```
,,,
$ ,date >> dateList,,
$ ,cat dateList,,
$ ,,write,/tmp/dateList.out
```

Instructions

Follow these steps to utilize a telnet_normalizer data collector:

1 The default properties file should be fine, but you can edit the *"/musr/rb/udnei/telnet_normalizer/telnet_normalizer.properties"* file.

Reference: For the list of parameters, see the "Properties" (p. 43)

2 Edit *"/musr/rb/udnei/telnet_normalizer/map.tcl"* and *"/musr/rb/udnei/telnet_normalizer/parse.tcl"* files.

Reference: For the list of parameters, see the "TCL Files" (p. 33)

END OF STEPS

Reference

See "Using an existing UDNEI Data Collector" (p. 11), "Modifying/Removing UDNEI Data Collector" (p. 13), and "Provisioning a network element instance" (p. 16) procedures.

□

Utilizing ssh_normalizer Data Collector

Purpose

The `ssh_normalizer` is a normalizer-like data collector which utilizes an ssh connection. The user has the ability to provide a TCL map and parse scripts. The fetcher in this data collector consumes commands created by the TCL map script and invokes appropriate ssh connection functions.

Ssh_normalizer data collector provides the possibility to collect the following parameters for a specified network element type and their respective values for network element instances of that type provisioned to the user:

- IP - IP number or host name.
- User - user name.
- Passwd - password.
- Periodicity - period for collecting data (allowed values are: 5, 15, 30, or 60 minutes)
- Offset - offset time to start collecting data in milliseconds.
- Timeout - Timeout value in milliseconds.
- AuthMethod - Authorization method (allowed values are: keys, userpass).
- PrivKeyLocation - Location of the private key. This parameter is optional, and overrides the location provided in the *ssh_normalizer.properties* file.
- Passphrase - Phrase used to decode the private key. This parameter is optional.
- Port - Allows using other port than default (22). This parameter is optional.
- ConnectionClass - Parameter to pass other implementation of the ssh protocol. This parameter is optional.

Ssh_normalizer_clli File Example

This is an example of populated ssh_normalizer_clli file:

```
paramName=IP,paramValue=meas_host,encrypted=n
paramName=User,paramValue=meas_user,encrypted=n
paramName=Passwd,paramValue=meas_passwd,encrypted=n
paramName=Periodicity,paramValue=15,encrypted=n
paramName=Offset,paramValue=0,encrypted=n
paramName=Timeout,paramValue=5000,encrypted=n
paramName=AuthMethod,paramValue=Keys,encrypted=n
paramName=PrivKeyLocation,paramValue=/musr/nmadm/.ssh/id_rsa,encrypted=n
paramName=Passphrase,paramValue= ,encrypted=n
```

`Important!` If in the *errors* file appeared one of the following errors:

```
Check User/PrivKeyLocation or execute 'manage_ssh testconn' to update
SSH keys
Check User/Passwd or execute 'manage_ssh testconn' to update SSH keys
```

1. Check the ssh_normalizer_clli file if the clli user/passwd or your own SSH keys were changed, and recreate the clli.

2. Execute `manage_ssh testconn` if the clli SSH keys were changed.

Properties

All the dcol parameters for `ssh_normalizer` must be provided in the *"/musr/rb/udnei/ssh_normalizer/ssh_normalizer.properties"* file. The properties file can be changed during DCOL process. It will be updated in the next 5-min. period. The "*udnei_ssh_normalizer.<#>"* log files reside under the *"/musr/tracer/"* folder. The following is the list of available parameters:

- kernel.threads - Number of parallel scan threads. The default is 1.
- kernel.retryInterval - Time between two connection/scan attempts for one network element in milliseconds. The default is 10,000 milliseconds. Maximum value is 280,000 milliseconds.
- kernel.logSize - Size of the log file. The default is 1,000,000.
- kernel.logRotate - Number of the log files. The default is 2.
- kernel.jobTimeout - job timeout in milliseconds - the maximum time allowed for a job execution. The default is 5000.
- kernel.logFormat - Format of the log files: TEXT or XML. The default is TEXT.
- kernel.logLevel - The logging level. One of the following option: NONE, SEVERE, WARNING, INFO, FINE, FINER, FINEST, ALL. The default is WARNING.
- kernel.logEntity - name of NE entity that log is filtered for, empty means log is not filtered
- defaultTimeout - default timeout for a single user command (in milliseconds).
- kernel.retries - the number of how many times failed job should be retried. The maximum value is 10.
- defaultSshPrivFile - default location of the ssh private keys.

TCL Files

Ssh_normalizer uses two files *map.tcl* and *parse.tcl*. File *map.tcl* is used for creating a sequence of commands for retrieving data. File *parse.tcl* is used for validation and processing of the retrieved data.

The syntax of the commands created by the map TCL script consists of multiple command lines of the following format:

```
Search string, Input, Action, FileName
```

`Search string`text to search for on the STDOUT of the ssh connect.

`Input` next “command” to write on the STDIN of the ssh connection.

`Action` field will be limited to {null|write|append}.

`FileName` local file to which the captured STDOUT data is written (or appended to).

Reference: All the parameters and examples of TCL files you can find in the Normalizer Data Collector section “TCL Files” (p. 16-33).

Example

The following is a set of command example from TCL script:

```
,,,
$ ,date >> dateList,,
$ ,cat dateList,,
$ ,,write,/tmp/dateList.out
```

Instructions

Follow these steps to utilize a ssh_normalizer data collector:

1 The default properties file should be fine, but you can edit the *“/musr/rb/udnei/ssh_normalizer/ssh_normalizer.properties”* file.

Reference: For the list of parameters, see the “Properties” (p. 47)

2 Edit *“/musr/rb/udnei/ssh_normalizer/map.tcl”* and *“/musr/rb/udnei/ssh_normalizer/parse.tcl”* files.

Reference: For the list of parameters, see the “TCL Files” (p. 33)

END OF STEPS

Reference

See “Using an existing UDNEI Data Collector” (p. 11), “Modifying/Removing UDNEI Data Collector” (p. 13), and “Provisioning a network element instance” (p. 16) procedures.

□

Utilizing SNMP Data Collector

SNMP Data Collector

The SNMP data collector provides the possibility to collect the data using SNMP interface. The 8920 NTM supports two types of SNMP interfaces:

- SNMPcom Data Collector - for Community-based SNMP version 1 and 2
- SNMPsec Data Collector - for Security-based SNMP version 3.

Each Network Element which uses SNMP interface requires file with access parameters. The SNMP access parameters are read at SNMP session initialization, which occurs at system start time and network activation time. The SNMP data collector monitors changes to access parameters and responds them by the next collection interval. For each DataSet at least one Input DataSet configuration file and one Output DataSet configuration file is required. Command `validate_snmp_dataset` can be used to validate the DataSet configuration files. When some data for specific interval is missing then SNMP Data Collector set the status of data as partial.

The Periodic Data Browser and Detail pages show the UDDM data types which are collected by the SNMP Data Collector. The associated Alerts are presented on the Alert Table and Alert Administration pages.

Community-based SNMP Parameters

The following are the access parameters for Community-based SNMP:

- URI - IP address in dotted decimal notation or DNS name and port number (typically port number is 161), includes udp/tcp protocol designation.
- SNMP Version - Allowed values: V1, V2C; the default value is V2C.
- Community - Community Name for identifying group of devices. The default value is public.

Security-based SNMP Parameters

The following are the access parameters for Security-based SNMP:

- URI - IP address in dotted decimal notation or DNS name and port number (typically port number is 161), includes udp/tcp protocol designation.
- SNMP Version - Allowed value is V3.
- Authentication Protocol - Allowed values: MD5, SHA; the default value is MD5.
- Privacy Protocol - Allowed values: DES, AES128, AES192, AES256; the default value is DES (CBC DES).
- Security Name - encrypted value.

- Authentication Passphrase - encrypted value.
- Privacy Passphrase - encrypted value.

Properties File

All the dcol parameters for `snmpcom` and `snmpsec` must be provided in the *“/musr/rb/udnei/snmpcom/snmpcom.properties”* and *“/musr/rb/udnei/snmpsec/snmpsec.properties”* file . The properties file can be changed during DCOL process. It will be updated in the next 5-min. period. The following is the list of available parameters:

- kernel.threads - Number of parallel scan threads. The default is 1.
- kernel.retryInterval - Time between two connection/scan attempts for one network element in milliseconds. The default is 10,000 milliseconds. Maximum value is 280,000 milliseconds.
- kernel.logSize - Size of the log file. The default is 1,000,000.
- kernel.logRotate - Number of the log files. The default is 2.
- kernel.jobTimeout - job timeout in milliseconds - the maximum time allowed for a job execution.
- kernel.logFormat - Format of the log files: TEXT or XML. The default is TEXT.
- kernel.logLevel - The logging level. One of the following option: NONE, SEVERE, WARNING, INFO, FINE, FINER, FINEST, ALL. The default is WARNING.
- kernel.logEntity - name of NE entity that log is filtered for, empty means log is not filtered.
- kernel.retries - the number of how many times failed job should be retried. The maximum value is 10.

Input DataSet Configuration File

Input DataSet configuration file contains the list of OIDs which should be collected on a periodic or demand basis. The information must be defined for each DataSet which will be collected. The Input DataSet file:

- */musr/rb/udnei/snmpcom/<inputDataset>.input.xml*
- *or /musr/rb/udnei/snmpsec/<inputDataset>.input.xml*

reside under dcol directory. The XML file must be consistent with the schema from *inputDataset.xsd* file.

The following configuration data is needed:

- DataSet Name – this name corresponds with a MIB table or list of scalars
- DataSet Type – The only allowed value is “input”.
- SNMP type - Allowed values: scalar list, table.

- counterResetOID – the OID to check to determine if counters were reset (e.g. sysUpTime). This OID will typically be of type TimeTicks.
- counterScale = Allowed values: yes, no – whether to scale counter values. Scaling is a method to alter the data if the collection interval is not consistent. The scaling calculation is: (previous value – current value) * (desired interval/actual interval). The actual interval should be calculated as the time since the last interval was received for this Input DataSet.
- snmpRetries – Number of retries. The default value is 0.
- snmpTimeout – Timeout value. The default value is 10 seconds.
- List of selection criteria (may be null). This is applicable only for table DataSets. If a selection criteria is specified, then the selection criteria lists the reference database table and fields to be used as the index to the OIDs to be selected:
  - Table.fieldname
- List of OIDs:
  - fieldname – this is the name with which to access the field by the Data Collector
  - OID – the OID to retrieve excluding the index values
  - Key - Allowed values: yes, no.
  - SNMP data type
  - Enumeration name if applicable

Important! Note that a DataSet may not contain both scalars and tables. This is due to the fact that there is only one instance of each scalar value, but there may be multiple rows of the table values.

Input DataSet Examples

Following is the example of the *<inputDataset>.input.xml* file with scalar list:

```
<dataset name="bwapplretry" type="input">
  <counterResetOID>1.3.6.1.2.1.1.3.0</counterResetOID>
  <counterScale>false</counterScale>
  <snmpRetries>3</snmpRetries>
  <snmpTimeout>10000</snmpTimeout>
  <scalarList>
    <variable name="bwSipStatsMsgRetryIndex"
   oid="1.3.6.1.4.1.6431.1.2.9.1.53.1.1.<value1>" type="Integer32"/>
    <variable name="bwSipStatsMsgRetryToNeAddr"
   oid="1.3.6.1.4.1.6431.1.2.9.1.53.1.2.<value1>" type="DisplayString"/>
    <variable name="bwSipStatsMsgRetryToNePercentage"
   oid="1.3.6.1.4.1.6431.1.2.9.1.53.1.3.<value1>" type="Gauge32"/>
  </scalarList>
</dataset>
```

Following is the example of the *<inputDataset>.input.xml* file with scalar list:

```
<dataset name="bwapplretry" type="input">
  <counterResetOID>1.3.6.1.2.1.1.3.0</counterResetOID>
  <counterScale>false</counterScale>
  <snmpRetries>3</snmpRetries>
  <snmpTimeout>10000</snmpTimeout>
  <table>
    <index name="bwSipStatsMsgRetryIndex"
   oid="1.3.6.1.4.1.6431.1.2.9.1.53.1.1" type="Integer32"/>
    <variable name="bwSipStatsMsgRetryToNeAddr"
   oid="1.3.6.1.4.1.6431.1.2.9.1.53.1.2" type="DisplayString"/>
    <variable name="bwSipStatsMsgRetryToNePercentage"
   oid="1.3.6.1.4.1.6431.1.2.9.1.53.1.3" type="Gauge32"/>
  </table>
  <selection>
    <indexValue name="bwSipStatsMsgRetryIndex" values="1,2,3"/>
  </selection>
</dataset>
```

Output DataSet Configuration File

Output DataSet configuration files contain the mapping of Input DataSets to the NTM datatype. The information must be defined for each DataSet which will be produced. The Output DataSet files reside under the dcol directory: */musr/rb/udnei/snmpcom/* or */musr/rb/udnei/snmpsec/*. The SNMP Data Collector looks for the following file names:

- *periodic.<datamodel>.output.xml*
- *periodic.<datamodel>.<entid>.output.xml*
- *periodic.<datamodel>.<udnei>.<generic>.output.xml*
- *periodic.<datamodel>.<udnei>.output.xml*

The XML files must be consistent with the schema from *outpuDataset.xsd* file. The following configuration data is needed:

- DataSet Name – the name of the NTM datatype (UDDM type)
- DataSet Type - The only allowed value is “output”.
- List of Input DataSets:
  - Input DataSet Name – this is one of the DataSets where the fields originate.
- sql - SQL query to retrieve data from input Dataset table.

Output DataSet Examples

Following is the example of the *<datamodel>.output.xml* file:

```
<dataset type="output" name="bwapplretry">
        <inputDatasets>
                <dataset name="bwapplretry"/>
        </inputDatasets>
        <sql>select * from bwapplretry</sql>
```

```
</dataset>
```

Jobs Timeout

The Data Collector timeout can be defined for:

- dcol task - collecting one type (data model) of periodic data, or one type of audit/control.
- dcol job - collecting periodic data from one network element (can contain few tasks) or executing audit/control (this is always one task).

Maximum time for finishing one job is defined in the properties file as a `kernel.jobTimeout` parameter (Properties File). Each dcol has separate timeout for SNMP connection, hovewer the job timeout has greater priority. In case of failure or timeout, specific job will be executed again after the time defined in the `kernel.retryInterval` parameter.

For snmpcom and snmpsec Data Collectors user can change the TimeOut value of specific jobs (periodic, audit, and control). The timeout value (in milliseconds) must be prepared for a ‘job’ node in the */musr/rb/udnei/<dcol>/periodic.xml* file. Following is an example line from the *<job>.xml* file:

```
<job name="<jobname>" timeout'"20000">
```

This timeout applies to only one task, so in case of periodic data it will be multiplied by the number of collected models.

Instructions For SNMPcom

Follow these steps to utilize a SNMPcom Data Collector:

1 Create and edit the *“/musr/rb/udnei/snmpcom/<inputdataset>.input.xml”* file.

Reference: For the list of parameters, see the “Input DataSet Configuration File” (p. 50)

2 Create and edit *“/musr/rb/udnei/snmpcom/<datamodel>.output.xml”* file.

Reference: For the list of parameters, see the “Output DataSet Configuration File” (p. 52)

3 Optionally validate correctness of configuration files executing

```
validate_snmp_dataset -input <inputdataset>.input.xml
validate_snmp_dataset -output <datamodel>.output.xml
```

END OF STEPS

Instructions For SNMPsec

Follow these steps to utilize a SNMPsec Data Collector:

1 Create and edit the *"/musr/rb/udnei/snmpsec/<inputdataset>.input.xml"* file.

Reference: For the list of parameters, see the "Input DataSet Configuration File" (p. 50)

2 Create and edit *"/musr/rb/udnei/snmpsec/<datamodel>.output.xml"* file.

Reference: For the list of parameters, see the "Output DataSet Configuration File" (p. 52)

3 Optionally validate correctness of configuration files executing

```
validate_snmp_dataset -input <inputdataset>.input.xml
validate_snmp_dataset -output <datamodel>.output.xml
```

END OF STEPS

Reference

See "Using an existing UDNEI Data Collector" (p. 11), "Modifying/Removing UDNEI Data Collector" (p. 13), and "Provisioning a network element instance" (p. 16) procedures.

□

Utilizing SOAP Data Collector

Before you begin

To start working with SOAP Data Collector the user must be acquainted with:

- XML - Extensible Markup Language,
- XSLT - Extensible Stylesheet Language Transformations ver.1.0,
- XSD - XML schema definition,
- XPath - XML Path Language,
- SOAP protocol.

SOAP Data Collector

The SOAP data collector provides the possibility to collect the data from Network Elements using SOAP interface. The NTM supports SOAP interface version 1.1 and 1.2.

Each Network Element which uses SOAP interface requires file with access parameters. The SOAP parameters are read at SOAP session initialization, which occurs at system start time and network activation time. The SOAP data collector monitors changes to the parameters file and responds them by the next collection interval.

At every step of action, SOAP Data Collector works with a pair of XML and XSLT files which are transformed into one XML:

- configuration data (Configuration Files),
- request message (Request File),
- error message (Errors File),
- response message (Response File).

The Periodic Data Browser and Detail pages show the UDDM data types which are collected by the SOAP Data Collector. The associated Alerts are presented on the Alert Table and Alert Administration pages.

Properties File

The file *soap.properties* which configures the SOAP data collector globally is located in the */musr/rb/udnei/soap/* directory. The following is the list of parameters for this file:

- kernel.threads - number of parallel threads executing data collection jobs
- kernel.retryInterval - time in milliseconds between two attempts of a job execution in case of conntimeout, readtimeout, or jobTimeout (see:Configuration File Parameters).

- kernel.jobTimeout - job timeout in milliseconds - the maximum time allowed for a job execution (job - collects all periodic data models for one entity within a period; or executes one audit/control request for one entity)
- kernel.logSize - Maximum size for the log file.
- kernel.logRotate - Number of log files in rolling archive.
- kernel.logFormat - Format of log files (TEXT or XML)
- kernel.logLevel - Level for log files (NONE, SEVERE, WARNING, INFO, FINE, FINER, FINEST or ALL)
- kernel.logEntity - name of NE entity that log is filtered for, empty means log is not filtered
- kernel.retries - the number of how many times failed job should be retried. The maximum value is 10.

Access Parameters

The parameter file named the same as the Network Element must exist in the */musr/rb/udnei/soap/<UDNEIType>* folder. The file contains following parameters:

- user - authentication name
- passwd - authentication password
- url - IP address of the Network Element, service port number, and service path
- key_store - Path to the keystore file.
- store_password - Password to the keystore file.
- endpointip - Defines SQL query. Exclusive for the NexTone Network Element.

Configuration Files

To configure SOAP Data Collector for collecting periodic data you must prepare a pair of XML and XSLT files under the */musr/rb/udnei/soap/<UDNEIType>/<generic>* directory (list is presented in a priority which SOAP dcol uses the files):

- *<UDDMType>.<clliname>.config.xml*, and *<UDDMType>.<clliname>.config.xslt*
- *<UDDMType>.config.xml*, and *<UDDMType>.config.xslt*

To configure SOAP Data Collector for collecting audits you must prepare a pair of XML and XSLT files (list is presented in a priority which SOAP dcol uses the files):

- *audit.<auditname>.<clliname>.config.xml*, and *audit.<auditname>.<clliname>.config.xslt*
- *audit.<auditname>.config.xml*, and *audit.<auditname>.config.xslt*

To start collecting control data using SOAP Data Collector you must prepare a pair of XML and XSLT files (list is presented in a priority which SOAP dcol uses the files):

- *control.<controlname>.<clliname>.config.xml*, and *control.<controlname>.<clliname>.config.xslt*
- *control.<controlname>.config.xml*, and *control.<controlname>.config.xslt*

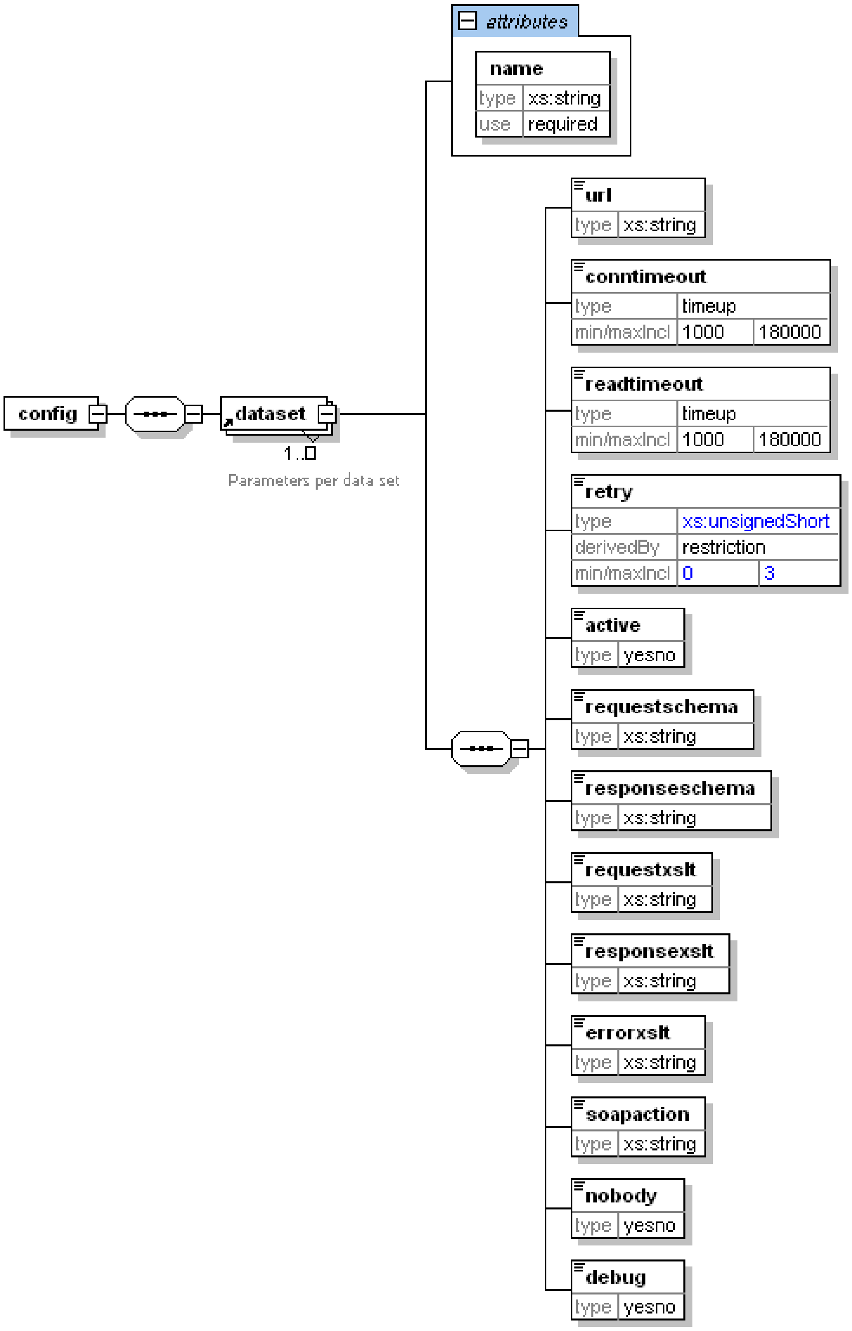
Important! If under */musr/rb/udnei/soap/<UDNEIType>/<generic>* directory exist *<UDDMType>.<clliname>.config.xml* and *<UDDMType>.config.xml* files then SOAP dcol will use the file which has greater priority: *<UDDMType>.<clliname>.config.xml*.

SOAP dcol uses these files to produce configuration file *"<period>.<UDDMType>.<clliname>.config.xml"* for specific period. When the debug flag is set to `yes` this file is stored in the */musr/swdata/udnei/<UDNEIType>* directory. The XML and XSLT files must be prepared using correct sets of parameters that configuration file which will be produced is consistent with the schema from *ntmconfig.xsd* file (Figure 2).

Configuration File Diagram

Figure 2 presents the *ntmconfig.xsd* schema.

Figure 2 Config schema diagram



Configuration File Parameters

According to schema presented in the *ntmconfig.xsd* file you can set following parameters:

- name - Dataset name.
- url - IP address of the Network Element, service port number, and service path

- conntimeout - Connection TimeOut in milliseconds (range for allowed value is: 1000 - 18000).
- readtimeout - Read Data TimeOut in milliseconds (range for allowed value is: 1000 - 18000).
- retry - Value for allowed retries. This value represents how many times the dcol will try to get the data after `readtimeout` or `conntimeout` (range for allowed value is: 0 - 3).
- active - DataSet activation. Allowed values: yes, no.
- requestschema - Schema file for request.xml file. If not provided dcol will not validate request files.
- responseschema - Schema file for response.xml file. If not provided dcol will not validate response files but they will be parsed by the SOAP dcol.
- requestxslt - request.xslt file which is used with request.xml file. (Request File)
- responsexslt - response.xslt file which is used with the response from the Network Element.
- errorxslt - error.xslt file which is used with the response from Network Element (Errors File). SOAP Data Collector produce the XML file according to the schema from the *ntmerror.xsd* file.
- soapaction - soapaction value from the WSDL file.
- nobody - Allowed values: yes, or no. If set to “yes” you do not have to provide the `requestxslt` file. The SOAP dcol connects to the Network Element using http GET method and downloads WSDL files from the switch.
- debug - Allowed values: yes, or no. If set to “yes” debug files is written to */musr/swdata/udnei/<UDNEIType>* directory such like requests, responses, etc.

Request File

To collect the specific data using SOAP interface you must prepare request files. Similar to the configuration files this is a pair of XML and XSLT files. The name of the XSLT file is written in the configuration file as a `requestxslt` parameter. The XML request file which SOAP Data Collector uses with the `requestxslt` file has the following name (list is presented in a priority which SOAP dcol use the file):

- <Dataset_name>.*<clliname>.request.xml*
- <Dataset_name>.*<clliname>.request.xml*
- <Dataset_name>.*request.xml*

The file which is produced from XML and XSLT files is validated with the `requestschema` file if given. When `requestschema` file is not available then request file will be sent to the Network Element without validation. If request does not match the schema request will not be send to the switch, and on the dcol status page following error is displayed: “`Request doesn’t match schema`”.

Errors File

Before getting the response from Network Element, you have to prepare a file which will be used for generating errors. The file given in the `errorxslt` parameter of the configuration file must be written according to the schema from *ntmerror.xsd*. The following is an example line from the produced schema:

```
<error> error_message <\error>
```

When `error_message` is “ok” (text is not case sensitive) the response message from Network Element is considered as correct. If the `error_message` is not “ok” then the data is not processed and `error_message` is written into the errorlog and dcol status.

Response File

After receiving XML data from Network Element, SOAP Data Collector uses XSLT file provided in the configuration file as the `responsexslt` parameter. The `responsexslt` file must be created with correct set of parameters that SOAP dcol transforms the received XML data into the following format:

```
<data>
      <row>
            <column_name> received_data <\column_name>
            ...
      <\row>
      ...
<\data>
```

Then SOAP dcol is processing the data into CSV file in the */musr/hod/<UDNEIType>/<UDDMtype>* directory.

XSLT General Parameters

The following is the list of general parameters for all XSLT files:

- Every parameter from the initialization parameter file:
  - user - authentication name
  - passwd - authentication password
  - url - IP address of the Network Element, service port number, and service path
  - key_store - Path to the keystore file.

  - store_password - Password to the keystore file
  - endpointip - Defines SQL query. Exclusive for the NextOne Network Element.
- begindate - The beginning of a period date in specific format: YYYY-MM-DDTHH24:mm:ss.tZ (GMT Timezone)
- enddate - The end of a period date in specific format: YYYY-MM-DDTHH24:mm:ss.tZ (GMT Timezone)
- begindate2db - The beginning of a period minus 48 hours in format: YYYY-MM-DD HH24:mm:ss (GMT Timezone)
- period - The beginning of a period in Linux format.
- date - The beginning of a period in format: YYYY-MM-DD HH24:mm:ss (GMT Timezone)
- entid - Network Element name

Jobs Timeout

The SOAP Data Collector timeout can be defined for:

- dcol task - collecting one type (data model) of periodic data, or one type of audit/control.
- dcol job - collecting periodic data from one network element (can contain few tasks) or executing audit/control (this is always one task).

Maximum time for finishing one job is defined in the properties file as a `kernel.jobTimeout` parameter (Properties File). Each dcol has separate timeout for SOAP connection, hovewer the job timeout has greater priority. In case of failure or timeout, specific job will be executed again after the time defined in the `kernel.retryInterval` parameter.

For SOAP Data Collectors user can change the TimeOut value of specific jobs (periodic, audit, and control). In the appropriate file:

- */musr/rb/udnei/soap/periodic.xml*
- */musr/rb/udnei/soap/audit.xml*
- */musr/rb/udnei/soap/control.xml*

the timeout value (in milliseconds) must be prepared for a ‘job’ node. Following is an example line from the <*job*>*.xml* file:

```
<job name=”<jobname>” timeout’”20000”>
```

This timeout applies to only one task, so in case of periodic data it will be multiplied by the number of collected models.

Instructions

Follow these steps to utilize SOAP Data Collector:

1 If you are using HTTP secure connection prepare keystore file.

Reference: See the "Creating Keystore File" (p. 16-64)

2 create */musr/rb/udnei/soap/<UDNEIType>/<clliname>* parameters file.

Reference: See the "Access Parameters" (p. 16-56)

3 create configuration XSLT and XML files under the */musr/rb/udnei/soap/<UDNEIType>/<generic>* directory.

Reference: See the "Configuration Files" (p. 16-56)

4 create request XSLT and XML files as provided in the configuration file under the */musr/rb/udnei/soap/<UDNEIType>/<generic>* directory.

Reference: See the "Request File" (p. 16-59)

5 copy XSD request and response schema files to the */musr/rb/udnei/soap/<UDNEIType>/<generic>* directory.

Reference: See the "Configuration File Diagram" (p. 16-57)

6 create error XSLT file as provided in the configuration under the */musr/rb/udnei/soap/<UDNEIType>/<generic>* directory.

Reference: See the "Errors File" (p. 16-60)

7 create response XSLT file as provided in the configuration file under the */musr/rb/udnei/soap/<UDNEIType>/<generic>* directory.

Reference: See the "Response File" (p. 16-60)

END OF STEPS

Reference

See “Using an existing UDNEI Data Collector” (p. 11), “Modifying/Removing UDNEI Data Collector” (p. 13), and “Provisioning a network element instance” (p. 16) procedures.

□

Creating Keystore File

Purpose

The `keystore` file contains certificates for the secure HTTP connections. You have to add certificate for every Network Element you are using with secure connection. This file is encrypted with password provided as a *`keystore_pass`* parameter in the access parameters file. To create or update keystore file use the `keytool` command located in the */nm/jdk/bin/* folder.

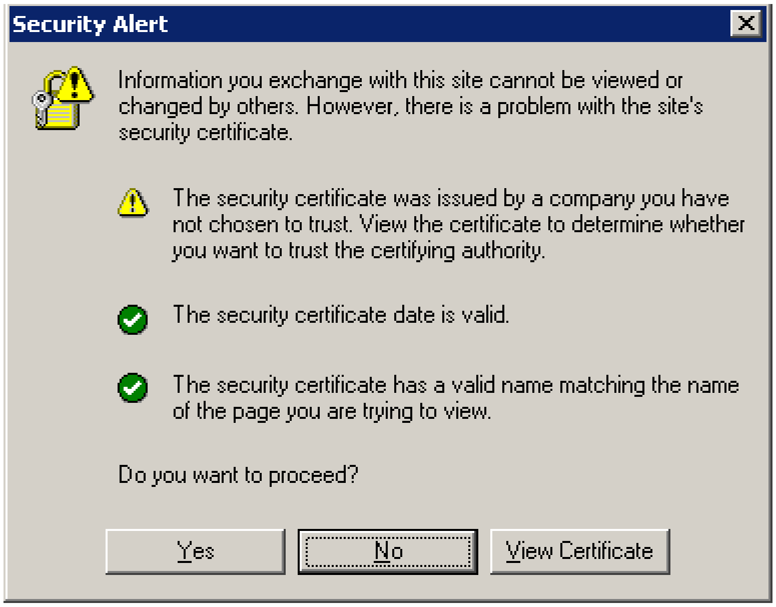
Instructions

Follow these steps to add the certificate to the keystore file:

1 Connect to the Network Element and download certificate file.

Important! Steps from 2 to 6 show the process of downloading the file from nextone switch using Internet Explorer 6 browser.

2 Open Internet Explorer and connect to the switch. The Security Alert popup window should appear. On this window click `View Certificate` button.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

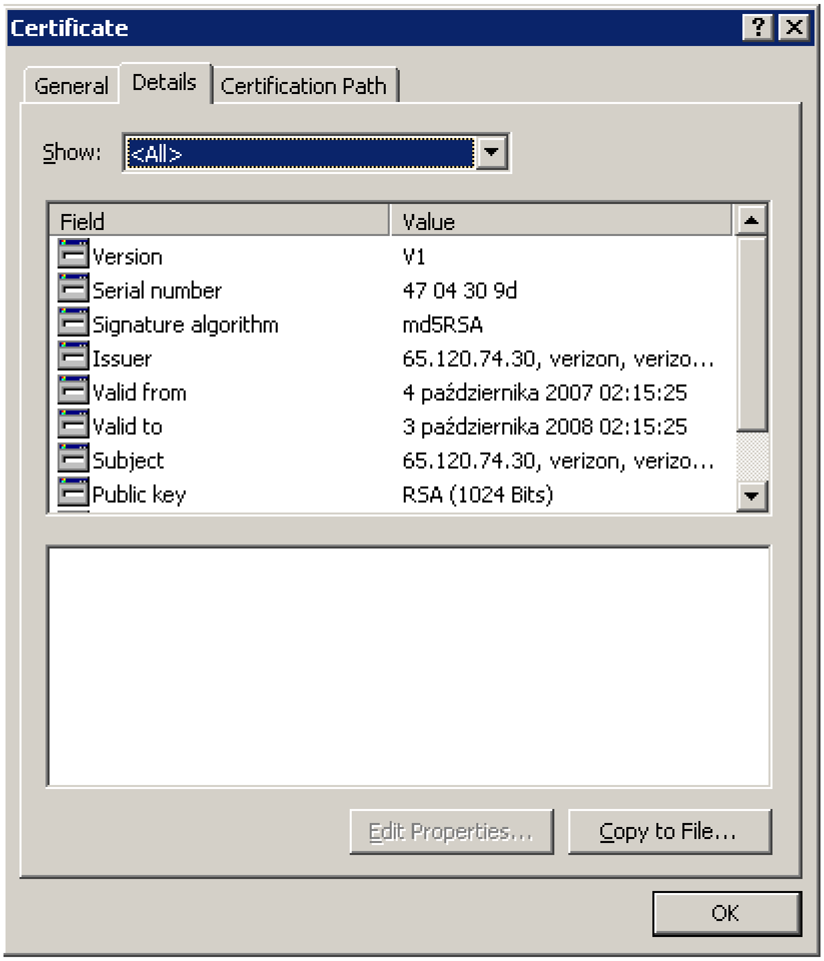
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

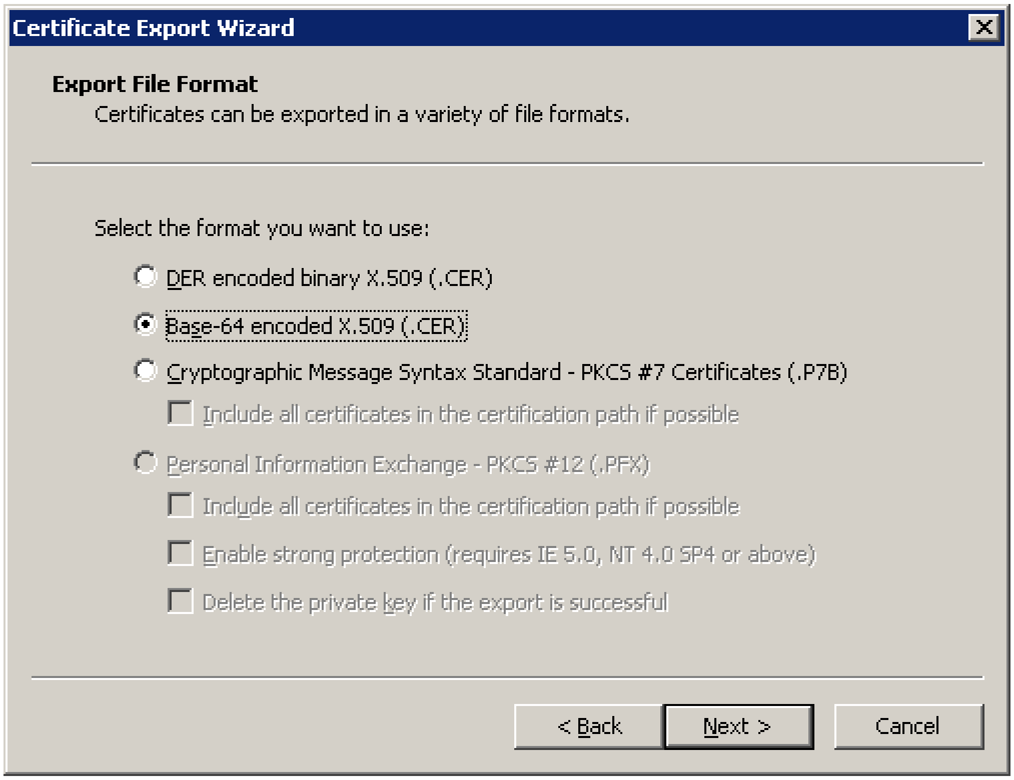
Do you want to proceed?

3 Go to the `Details` tab in the Certificate window and click `Copy to File...` button.



Field	Value
Version	V1
Serial number	47 04 30 9d
Signature algorithm	md5RSA
Issuer	65.120.74.30, verizon, verizo...
Valid from	4 października 2007 02:15:25
Valid to	3 października 2008 02:15:25
Subject	65.120.74.30, verizon, verizo...
Public key	RSA (1024 Bits)

4 Click `next` on the Certificate Export Wizard welcome screen then on the Export File Format screen choose the `Base-64 encoded X.509 (.CER)` option and click `next` button.



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

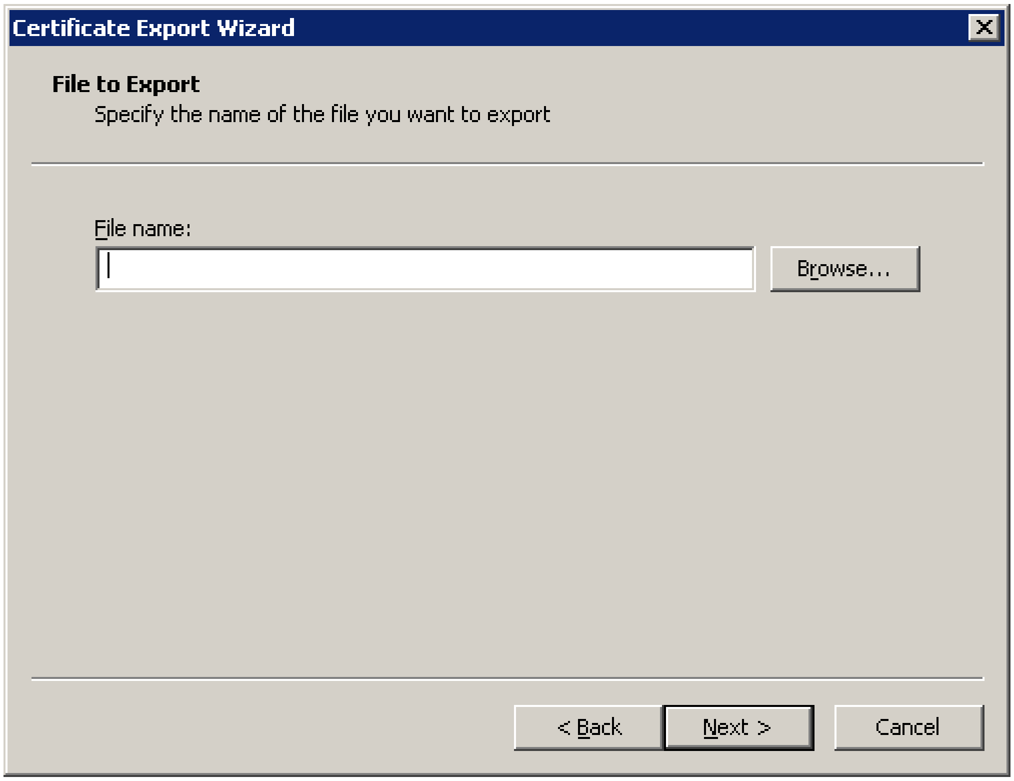
○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

5 Specify the name of the certificate file and click `next` button.



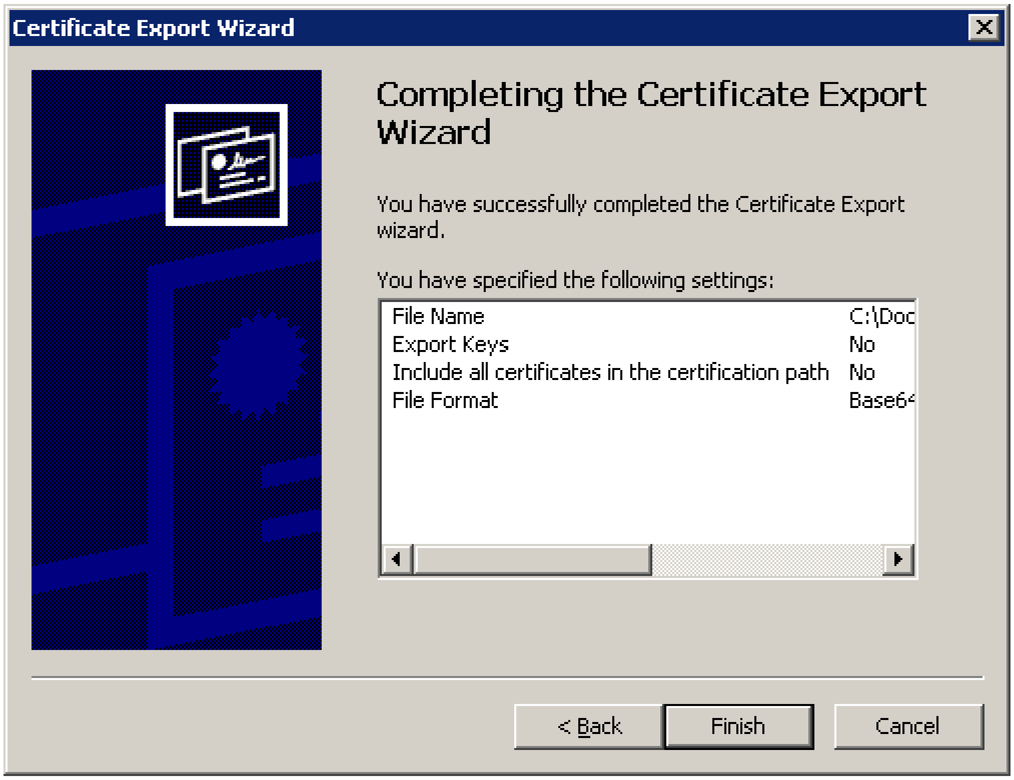
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

6 Review the settings and click Finish to save the certificate file.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Doc
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

7 Copy the certificate file to NTM machine.

8 Execute `keytool -import -trustcacerts -alias alias_name -file mycertificate.cer -keystore keystore.file`

Important! Remember to provide full path to certificate and keystore files.

9 Provide the password for the keystore file. If the keystore file exists provide existing password if not the file will be created with the password you have provided.

10 Answer “y” for the question: `Trust this certificate?`

Example: Following is the example output for the `keytool` command.

```
$ /nm/jdk/bin/keytool -import -trustcacerts -alias nextone -file
   ./nextone.cer -keystore ./store2.trust
Enter keystore password:  123456
```

```
Owner: CN=192.168.74.30, OU=verizon, O=verizon, L=baltimore, ST=md, C=us
Issuer: CN=192.168.74.30, OU=verizon, O=verizon, L=baltimore, ST=md,
   C=us
Serial number: 4704309d
Valid from: Wed Oct 03 20:15:25 EDT 2007 until: Thu Oct 02 20:15:25 EDT
   2008
Certificate fingerprints:
         MD5:  FF:FF:FF:00:00:00:00:00:00:00:FF:FF:FF:EE:FF:00
         SHA1:
   FF:DD:DF:FF:FF:D2:A1:A2:A1:FF:FF:FF:FF:B6:81:EE:CE:CE:00:A3
Trust this certificate? [no]:  y
Certificate was added to keystore
```

11 Repeat steps 1 to 10 for every switch you want to configure.

12 Add path and password to the keystore file as a *key_store* and *store_password* parameters into the access parameters file.

Reference: See access parameters for SOAP data collector (Access Parameters)

END OF STEPS

□

Enhanced Thresholding and Analysis

Overview

Purpose

The main function of NTM is to collect periodic data from network elements about network objects. For each object for each period of data collection, the data is subjected to threshold tests and failed threshold tests are reported as alerts on various GUI screens. In general, you must decide how to react to those alerts. The Feature 437, “Enhanced Thresholding and Analysis” helps in analyzing the thresholded data.

The Feature 437, “Enhanced Thresholding and Analysis” consists of two parts. The first part is a framework for adding new event analysis jobs. The second is the jobs themselves. The framework is comprised of a set of software that understands that a set of event analysis jobs have been defined. Its function is to ensure that:

- these jobs get executed,
- any alerts generated from these jobs get posted to the GUI, and
- the jobs terminate gracefully.

Prerequisition

The Feature 436, “UDDM/UDNEI” must be purchased. The following tasks depend on this feature:

- The target table for the analysis results needs to be created.
- The threshold and reference files need to be created, populated, and loaded into Oracle.
- CC rules need to be written to process the files produced by the analysis.

Contents

This section contains the following topics:

□

How to initialize job

Purpose

To start a new analyzing job the executioner process must be properly configured. The configuration files, <UDDMType>_dat, <UDDMType>_ref, <UDDMType>_thr, <UDDMType>_cc, and executable job files must be prepared.

Executioner Process

The executioner works as a daemon process. When EOP message appears then it reads the configuration file (*"musr/udjobs/conf"*), job file ("*/musr/udjobs/jobList*") and "*/nm/udbin"* directory. The executioner starts the jobs in order specified in the jobList file according frequency value.

For a proper work of executioner, the following directories must exist in the system:

- /nm/udbin - contains all the executable job files
- /musr/udjobs - contains all the configuration job files

Log File

The executioner creates "musr/udjobs/log.<date>" file needed for further analysis. The log file contains:

- Status of finished jobs (completed, failed, killed, and so on).
- List of jobs that have not started.
- List of job that failed to start.
- Errors or problems with parsing the configuration file.

Configuration File

The "/musr/udjobs/conf/" file consist of the following parameters:

- MAX_PARALLEL_JOBS - maximum number of jobs run in parallel. The value is restricted to the range 2 - 16.
- Sleeping - argument for the sleep function. This value is restricted to the range 1- 10 sec.
- LogRollback - number of log files in rolling archive. The value is restricted to the range 1 - 10.
- Lines started with "#" are comments.

Configuration File Example

The following lines show the example of the *"musr/udjobs/conf"* file:

```
# MAX_PARALLEL_JOBS - how many jobs can run in parallel
# Sleeping - argument of sleep function
# LogRollback - number of log files in rolling archive
MAX_PARALLEL_JOBS=16
Sleeping=2
LogRollback=3
```

Job List File

The "*/musr/udjobs/jobList*" file contains maximum 100 jobs and each Job name is restricted to 100 characters. The "*/musr/udjobs/jobList*" file consists of the following parameters:

- NameOfJob - name of job. The same as the appropriate executable file in the *"/nm/udbin"* directory.
- Frequency - frequency value. The following values are allowed: 5, 15, 30, 60.
- MAX_JOB_TIME - maximum time for a job to run. The value is restricted to the range of 5 - 45 sec.
- SleepTerm - maximum time that the job is working after receiving SIGTERM. If job did not finish within SleepTerm time, SIGKILL is sent to the job process. This value is restricted to the range of 0 - 10 sec.
- UDDMType - name of UDDMType of up to 30 characters. This name is populated into csv file for jobstatus. This UDDMType is visible in the `Data Type` List on the Periodic Data Browser search page.
- Lines started with "#" are comments.

Important! Each job in the "*/musr/udjobs/jobList*" must be in separate line.

JobList Example

The following lines show the example of the "*/musr/udjobs/jobList*" file:

```
#Specify name of job then frequency value and MAX_JOB_TIME and SleepTerm
#NameOfJob Frequency MAX_JOB_TIME SleepTerm UDDMType
CODE_EVENT 5 15 5 CodeEvent
24HOUR_OFL 5 20 5 TG24HourOfl
MyJob1 30 10 5 UDtype
MyJob2 60 5 5 UDtype2
MyJob3 15 10 2 UDtype
```

Checking Status

Status for all new jobs is stored in a related UDDM table. The Periodic Data Browser page shows all the information and statuses for the jobs. If the general page contains no data for the individual job, then you can find more information on the Detail page for related UDDM type.

□

Setting job

Purpose

The executioner periodically starts jobs listed in the "*/musr/udjobs/jobList*" file. Jobs can be any executable file written in any script like perl, shell, or any binary file. The output of specific job is written in the directory *"/musr/hod/<UDDM_Job_Type>"* for further processing.

Initial Parameters

Current period is an argument for the job process. It is provided as 2 parameters in the following format:

- MM/DD/YYYY HH:MI
- Number of seconds since the Epoch.

Exit Parameters

All job processes must end with one of the following value passed to the "exit" function:

- Zero (0) - job finished correctly,
- 1 to 251 - exit codes provided for specific job,
- 252 - next eop arrived and job did not start,
- 253 - job received SIGTERM,
- 254 - feature is disabled,
- 255 - job did not start.

Instructions

Follow these steps to run a new job:

1 If needed create <UDDMType>.

Reference: See: "Creating a UDDMType" (p. 8).

2 Optionally edit *<UDDMType>_ref.template* file and save as *<UDDMType>_netevent* in the *"musr/rb/uddm"* directory.

3 Execute `create netevent`

4 Add job binary file to the *"/nm/udbin"* directory.

5 Change rights of the binary job file to: `-rwx------ nmadm snm`

6 Add new entry in the *"/musr/udjobs/jobList"* file.

Reference: See the "Job List File" (p. 74)

7 Executioner starts the job after the next EOP message according to the Frequency value specified in the *"/musr/udjobs/jobList"* file.

END OF STEPS

□

Code Event Analysis

Purpose

The Code Event Analysis job adds the ability to alert the network manager when Code Controls calling event actually begins or ends. This analysis job allows network managers to be alerted as to when a calling event begins (and ends) if they so desire and is also provides with information with which to assess the overall size of the event and effectiveness of the control.

This job enables defining thresholds on code controls existing in the network. On a per code basis, the network manager can set thresholds in a manner as is described in Feature 189, “Replacement Thresholding Capability for Trunk Group Data”. That feature allows for multi-level threshold testing, compound expressions, and scheduling of threshold rules.

Description

Operationally, for each period, the NTM aggregates the code control periodic data across all network elements, grouping by code. The network totals for this period for attempts, successes, and blocks may then be subject to threshold tests. If any threshold test fails, the system generates a new code event alert or it updates an existing alert. For a new alert, the event start time is set to the value of the current period. Total event values for attempts, successes, and blocks is set equal to the values of this first period. If an alert already is on-going, the event totals for attempts, successes, and blocks is incremented with the current period’s values. If all threshold tests pass, then the system will either close out an existing alert if one exists by setting the stop time in the record or do nothing. The system fully handles the case where there is an existing alert on a particular code and no data is received on that code in the current period. In this case, the alert on that code can be closed out. Total event values for attempts, successes, and blocks do not influence the Start_time or Stop_time of the event.

UDDM type

For Code Event Analysis job purposes, ***CodeEvent*** UDDM Type has been defined.

Exit Codes

The following are the exit codes for the Code Event Analysis job:

1 - wrong number of arguments is passed to the Code_event.sh script.

2 - failed to create *“/musr/hod/codeevent/<period>.CodeEvent.CodeEvent_dat”* file.

□

24-Hour Final TG Overflow Event Analysis

Purpose

Final Trunk Groups (TG) are the last in the chain used in the routing of calls. When they overflow, the calls are lost to the network. When 5-minute thresholds are exceeded, alerts are issued and results can be seen on the TG exception page in current NTM. When overflows are “constantly significant”, but maybe not over the 5-minute threshold often (if at all), it would be useful to detect such a condition. This feature allows the specification of a threshold that can be applied to the 24-hour total overflows on any final TG. Every 5 minutes, when the tg data is received from the network elements, the NTM system sums tg_ofl filed for the last 24 hours for this TG. Anytime the summation of the tg_ofl fails thresholds, the NTM system generates an alert.

Description

The NTM system is checking if this alert is a new or pre-existing. If this alert is new a “start time” is associated with the alert. If this alert is a pre-existing condition nothing is updated for the “start time”. This ensures that the original “start time” is kept or maintained until the tg overflow alert no longer exists. The stop_time will be set to the value of the next period in which the sum of the tg_ofl does not fail its threshold test. Records which sum of tg_ofl does not fail its threshold test will not be stored in the database.

After executing `stopsys`, 24-Hour Final TG Overflow Event is reset and start counting tot_tg_ofl field from the beginning.

UDDM type

For 24-Hour Final TG Overflow Event job purposes ***TG24HourOfl*** UDDM Type has been defined.

Exit Codes

The following are the exit codes for the 24-Hour Final TG Overflow Event job:

1 - wrong number of arguments is passed to the 24Hour_Ofl.sh script.

2 - failed to create *“/musr/hod/tg24hourOfl/<period>.TG24HourOfl.24HourOfl_dat”* file.

□

Mass Call Event

Purpose

With this Feature you can define on a system-wide basis, a mass calling event total threshold for the ssp_mass and ssp_ns counts. Every 5 min., when the mass call data is received from the network elements, the NTM system sums up across the network all the ssp_mass and ssp_ns data received. Anytime the summation of the ssp_mass and ssp_ns data received fails thresholds, the NTM system is generating an alert indicating the mass calling event has started.

Description

The NTM system is checking to see if this is a new or pre-existing mass calling condition. If this is a new mass calling condition, a “start time” is associated with the alert. If this is a pre-existing condition, nothing is updated for the “start time”. This ensures that the original “start time” is kept or maintained until the mass calling event no longer exists.

The analysis recognizes a Start_time for a mass call event as the period for which any of the threshold tests fail for the 5min. counts. The event is considered ongoing until a period occurs where no threshold tests fail for the 5min sums. At that time, the event is declared over and the Stop_time is populated.

During the lifetime of a mass call event, running totals is kept for ssp_ns and ssp_mass in tot_ssp_ns_event and tot_ssp_mass_event. These fields are subject to thresholding, but they do not influence the Start_time or Stop_time of the event.

UDDM type

For Mass Call Event job purposes ***MassCall*** UDDM Type has been defined.

Exit Codes

The following are the exit codes for the Mass Call Event job:

1 - wrong number of arguments is passed to the Mass_Call.sh script.

2 - failed to create *“/musr/hod/masscall/<period>.MassCall_dat”* file.

□

17 *Navis* Identity Software

Overview

Purpose

The *Navis*® Identity Software (*Navis* ID) Identity software provides centralized user management and common authentication. It reduces the effort required to manage user accounts and passwords for multiple *Navis*® iAssure software applications (e.g., NTM, NTM, and VitalSuite NTP). This feature allows users to have the same user account and password across all participating applications. It also performs user expiration checks, and ineffective attempts locking. The user's NTM specific preferences and permissions are maintained by the NTM host and are not affected by this feature.

This chapter contains information about the procedures done on the NTM side to enable, disable and configure the NTM system to function in a *Navis* ID environment, and the changes in the NTM GUI behavior as a result of enabling *Navis* ID.

Navis ID can run in two modes. The first is “common sign on”. In this mode, web users and, as an option, NTM command line access can use a common user name and password. This support is based on simple Radius server authentication. The second *Navis* ID mode is “single sign on”. In this mode, web users need only authenticate once to any systems that are participating in “single sign on”. This mode supports all of the functions of “command sign on”, for command line access.

Recommended time allotment for procedures

The following table provides approximate times required for each procedure in this chapter.

Procedure	Approximate Time Required	NTM Host	Report Writer Host
"Configuring Navis ID to interact with NTM" (p. 7)	15 minutes	X	
"Performing the initial upload to the Navis ID server" (p. 8)	15 minutes	X	
"Enabling Navis ID authentication for the Web GUI on the NTM host" (p. 10)	15 minutes	X	
"Enabling Navis ID authentication for NTM command line interface" (p. 13)	15 minutes	X	
"Bypassing Navis ID Web GUI authentication" (p. 16)	15 minutes	X	

Contents

This chapter contains the following topics:

□

Background

Overview

Purpose

The NTM features that support Navis ID are:

Feature 399, "Common Sign On"

Feature 407, "Single Sign On for NTM"

These features are only valid when used in an environment that provides a *Navis* ID server.

Multiple supported interfaces

By configuring the Command Line Interface (CLI) and Web GUI to authenticate against the same set of *Navis* ID servers, a user can use the same ID/password to access both types of interfaces. If *Navis* ID is used, applications can be configured to restrict user's to Web only, CLI only, or Web and CLI access on a per product basis.

Users must have matching logins and passwords on the *Navis* ID server and the NTM GUI for common sign on for the GUI interface. A user created on the *Navis* ID server must have a corresponding entry in the "/etc/passwd" file maintained on the NTM host for a log in to be successful. using the CLI.

The *Navis* Identity Software administrator must change the maximum allowable length of a login ID to accommodate the longest NTM user login. For example, the *Navis* default maximum login ID length of 10 characters is exceeded by the "administrator" login provided with NTM (which exceeds 10 characters).

Failure to do this will result in a mismatch in information between the two servers and the user will not be able to authenticate.

Initial migration

During the initial migration of the *Navis* ID feature or routine user administration you will need to perform the following:

- Configuring Navis ID to interact with NTM
- Enabling Navis ID authentication for NTM command line interface

Bypassing CSO authentication

During certain situations the Radius Server may be unavailable. If access is needed to the system, follow the steps below for authentication to the NTM System:

- “Troubleshooting” (p. 19)

References

For information about using the *Navis* ID product, see the *Navis® Identity Reference Guide* (255-178-300), provided with the *Navis* ID software.

□

Configuring NTM for a *Navis* ID environment

Overview

Purpose

There is initial configuring needed for NTM to successfully interact with Navis ID. This includes:

- "Configuring Navis ID to interact with NTM" (p. 7)
- "Performing the initial upload to the Navis ID server" (p. 8)
- "Enabling Navis ID authentication for the Web GUI on the NTM host" (p. 10)
- "Enabling Navis ID authentication for NTM command line interface" (p. 13)

Enabling and Disabling *Navis* ID Mode

Description

In some circumstances (for example, in case of hardware failure or network outage) it may be desirable to enable or disable the *Navis* ID feature.

> **Important!** Switching between *Navis* ID mode and Non-*Navis* ID mode should be performed with extreme caution, as it may render the system unusable if performed incorrectly.

Command syntax

Using the `navisidctl` command displays:

- current *Navis* ID status
- current state of the NTM *Navis* ID features and the NTM password aging features.

> **Important!** Password aging features should be disabled when running in the *Navis* ID mode.

- how to enable or disable *Navis* ID (-s and -d)

```
/nm/web/tools/deployment/navisidctl  [-e   -d   -s]
```

Command options are:

- `-e` – explains how to enable *Navis* Id mode
- `-d` – explains how to disable *Navis* Id mode
- `-s` – displays the status (display current mode, and displays associated NTM feature status.

> **Important!** If you attempt to enable/disable the feature when the feature is already enabled/disabled, you will receive a warning message.

Configuring *Navis* ID to interact with NTM

Purpose

All steps in this procedure must be performed on each NTM host that is to participate in the *Navis* ID environment.

Before you begin

During the time in which the NTM web server is stopped the GUI will be unavailable and user web requests will fail. It is best to coordinate this down time with users.

Instructions

Follow these steps to configure the *Navis* ID software to interact with NTM:

1 Log in to NTM as `root`.

2 On the NTM host, deactivate the PWA and EPWA features.

3 Activate the NTM *Navis* ID Feature 399, "Common Sign On" or Feature 407, "Single Sign On for NTM".

Result: The *Navis* ID Administrator can now configure each *Navis* ID server to operate with each NTM host.

Hint: Certain information used in configuring the Navis ID server will be used to configure the NTM host. Obtain the following from the Navis ID server:

- Shared secret
- Application ID

Important! Some NTM hosts may have more than one IP address assigned, be sure to configure the *Navis* ID server with all possible IP addresses for each NTM host.

END OF STEPS

□

Performing the initial upload to the *Navis* ID server

Purpose

This procedure describes how to allow the NTM users to be uploaded to the *Navis* ID Server. There are additional steps required by the *Navis* ID administrator on the Navis servers to complete this operation.

Instructions

If the current NTM users are to be migrated to the *Navis* ID server, follow these steps :

1 Log in to NTM as `root`.

2 Enter `cd /nm/web/tools/deployment`

3 To create a file that can be moved to the *Navis* ID Server, enter:

```
./export_ldap.pl <Application_ID> > <ntmusers>
```

Hint: The Application_ID is the application ID configured on Navis ID server in "Configuring Navis ID to interact with NTM" (p. 7).

Hint: The ntmusers file is created for Navis ID with NTM user information.

4 On the *Navis* ID Server, use the *Navis* ID bulk import tool to populate the user database with the NTM user list and their passwords.

5 If the Command Line Interface (CLI) of NTM is to authenticate user's using *Navis* ID, manually enter the CLI userid's into *Navis* ID using the *Navis* ID administrative Web GUI interface.

> **Important!** If another RADIUS server other than *Navis* ID is being used, use what ever local practices have been defined to add the Web and CLI user id's into the RADIUS server.

END OF STEPS

□

1

Enabling *Navis* ID authentication for the Web GUI on the NTM host

Purpose

All steps in this procedure must be performed on each NTM host that is to participate in the *Navis* ID environment.

2 On the NTM host, enable *Navis* ID authentication for the Web GUI by entering:

```
cd /nm/web/sup_soft/http/conf
```

3 Enter:

```
cp httpd.conf httpd.conf.<date>
```

This is a precautionary step.

4 Edit the file:

```
httpd.conf
```

> **Important!** You must know the following information from the *Navis* ID Server configuration discussed in Step 4 of "Configuring Navis ID to interact with NTM" (p. 7):
>
> - IP address(es)
> - shared secret(s)
> - Application ID
> - Name of the *Navis* ID server (SSO only)

5 To enable the "common sign on" mode, follow this step, if using "single sign on" proceed to Step 6.

To enable "common sign on", find the three locations in the server config file that are marked by the string "CSO SPOT 1/3", "CSO SPOT 2/3", and "CSO SPOT 3/3" and follow the instructions present in the file at each spot.

6 To enable the "single sign on" mode, find the two locations in the server config file that are marked by the string "Navis ID SPOT 1/2", "Navis ID SPOT 2/2" and follow the instructions present at each spot.

7 Save and exit the file.

8 Stop the web server:

```
../bin/stop-server
```

9 Start the web server:

```
../bin/start-server
```

Verify that Web User's can successfully authenticate through the NTM Web GUI.

Verify Web User's can access the *Navis* ID Web GUI using the same ID and password.

Result: The Web GUI should now be authenticating using RADIUS.

END OF STEPS

□

Command Line Interface (CLI) authentication

Purpose

The Command Line Interface (CLI) login process is configured to first check the *Linux “/etc/passwd”* file on the NTM host before attempting *Navis* ID authentication. In a situation where CSO authentication is inoperable a user can use the password already configured in the *“/etc/passwd”* entry. If a user's N password is locked (i.e. their password value is set to “*”) or can't be recalled, then the “root” user can reset the user's password using the “`passwd`” command.

Once the emergency has subsided, previously locked *Linux* level password's for user's can be locked again using the “passwd -l <id>” command.

> **Important!** Once locked at the *Linux* level, only the CSO password can be used for *Linux* level access.

References

For more information on the `passwd` command, consult the latest version of your *Linux* manuals.

Enabling *Navis* ID authentication for NTM command line interface

Instructions

Follow these steps to enable *Navis* ID authentication for the NTM command line interface:

1 Log in to NTM as `root`.

2 Edit:

```
/nm/etc/radius.conf
```

3 Follow the comments in the file.

The radius.conf file will contain the information regarding the IP address of the *Navis* ID servers and the shared secret.

4 Save and exit the file.

5 Enter:

```
cp /etc/pam.conf /etc/pam.conf.<date>
```

This is a precautionary step.

6 Enter:

```
cp /nm/etc/pam.conf.cso /etc/pam.conf
```

7 Edit:

```
/etc/pam.conf
```

8 Follow the comments in the file.

Hint: You will be substituting the NTM hosts Application ID assigned in Navis ID for the text “NTM_APPL_ID”.

9 Save and exit the file.

Result: CLI authentication will now try authenticating against the *“/etc/passwd”* entry for a user first, followed by *Navis* ID authentication, if needed.

10 Verify, in a separate terminal window, that the root user can access NTM using the *“/etc/passwd”* password.

11 Verify that a CLI user configured on the *Navis* ID server can access the CLI using their *Navis* ID password (Note: the user must exist in the *“/etc/passwd”* file for successful login)

END OF STEPS

□

Bypassing *Navis* ID authentication

Overview

Purpose

At times it is possible the *Navis* ID server will be un available. It may then be necessary to modify NTM to allow non-*Navis* ID authentication. This section covers:

“Bypassing Navis ID Web GUI authentication” (p. 16)

“Restoring normal Navis ID authentication after a bypass” (p. 18)

Bypassing Navis ID Web GUI authentication

Instructions

Follow these steps to bypass *Navis* ID Web GUI authentication:

1 Log in to NTM as `root`.

2 Enter:

```
cd /nm/web/sup_soft/http/conf
```

3 Edit the httpd.conf file, reversing the steps used in the "Enabling Navis ID authentication for the Web GUI on the NTM host" (p. 10).

Hint: If you created a precautionary backup file as instructed in Step 2 of "Enabling Navis ID authentication for the Web GUI on the NTM host" (p. 10) you can replace the config file with the backup.

4 Locate the section "Navis ID SPOT 2/2" in the httpd.conf file. Comment out the section beginning with <*IfModule mod_auth_navisid.c*> through the line <*/IfModule*>

Important! Customers may want to contact the Alcatel-Lucent customer support to assist in disabling the Navis ID feature.

5 Save and exit the file.

6 Execute:

```
./bin/stop-server
```

Result: This stops the Web Server.

7 Execute:

```
./bin/start-server
```

Result: This restarts the Web Server.

8 After by passing *Navis* ID authentication, NTM users may not have passwords. To restore the password for the default web “superuser”, enter

```
'/nm/web/tools/deployment/nmadm.pl clobber'.
```

Important! The password for the web user NetAdmin will be NetAdmin. This user can use used to restore passwords for any other users in the system.

END OF STEPS

□

Restoring normal Navis ID authentication after a bypass

Instructions

To re-enable *Navis* ID authentication after a bypass, repeat the procedures:

- "Enabling Navis ID authentication for the Web GUI on the NTM host" (p. 10)
- "Enabling Navis ID authentication for the Web GUI on the NTM host" (p. 10)

□

Troubleshooting

Overview

If the *Navis* ID authentication mechanism does not appear to be functioning properly check the following:

1. Have the *Navis* ID administrator verify the user's entry:
   - exists
   - is not locked
   - has permission for the corresponding application.
2. Verify the NTM host is identified as a valid client on the *Navis* ID server(s)
3. Verify that the shared secrets match between the *Navis* ID server(s) and the NTM host.
4. Verify the NTM host is configured with the proper IP address(es) of the *Navis* ID server(s)
5. Verify the NTM Web Server was restarted after modifications to the httpd.conf file.
6. Verify the communication between NTM and the *Navis* ID server(s) using "ping".
7. On the GUI, enter the URL: http(s)://<NTM hostname>/cgi-bin/guitst.pl. If successful a page is displayed showing the remote user ID, server name, etc. If unsuccessful an information screen may also be displayed indicating the user exists on the *Navis* ID server but not in the NTM host.
8. Verify the Application ID configured on NTM matches that configured on *Navis* ID server.

It is possible that a user id already exists having been created during a bulk import of user's in *Navis* ID. If so, the user already has a password assigned in *Navis* ID and that password will not be changed during another bulk import of user information.

It is also possible that a common ID (e.g., NetAdmin - the initial NTM Web GUI administration ID) may have already been assigned a password through a previous bulk import from another application. and when trying to access the NTM box using this ID access is not granted because the password being used is the NTM password not the current password set in *Navis* ID. This then gets complicated further because *Navis* ID can lock a user's account if an invalid password is entered on a set number of consecutive authentication attempts. This could then result in the account unintentionally being locked and access will be denied to all applications for this user ID.

□

18 Backup and Monitoring System Processes

Overview

Purpose

This appendix provides an overview of backup tools and a list of processes in NTM that can be monitored by optional third-party software to determine system reliability.

Contents

This appendix contains the following topics:

Tools used in backing up file systems and databases

Overview

Setting up RHEL backups use several utilities to backup file systems and the root disk. File system backups use the fbackup and frestore commands while the root disk backup is done by make_tape_recovery. Database backup is performed by the arcmanager utility.

> **Important!** The arcmanager script is installed under /nm/ubin directory. It is a user interactive command. Any effort to automate the database backup should include studying the /nm/ubin/arcmanager script.

The backup information from the NTM user documentation can be used in configuring other backup tools and utilities to automate the NTM recommended backups.

References

Chapter 5, "Backing Up and Restoring the System" has information on recommended backup schedule and backup scope information of file system, ROOT DISK and databases.

□

Monitoring NTM

Purpose

Certain NTM processes can be monitored by optional third-party software to determine system reliability.

Table 1 Monitoring Process

Process Name	Instances	Comments / Arguments	Intervals
The application related processes listed in the /etc/inittab file.	At least one	Monitor the NTM processes listed in the inittab file	30 minutes
/nm/sys/nminit	At least one	nminit respawns the NTM-related processes from the /nm/ubin/start.all file. While starting NTM processes nminit respawns itself. When the NTM processes are started, the nminit child processes are killed. nminit runs only when the system is running. Depending on the status of the application, the daemons are either running or not. When nminit is running, processes that are configured to respawn will respawn even if they are killed.	30 minutes
bin/httpd NTM release is 14.0 or later	At least one should be running. Ten server instances are started during system boot.	-D [Use PWA | No PWA] -D [NO_SSL | SSL_AND_NO_SSL | SSL_ONLY] -d /opt/apache -f /nm/web/sup_soft/http/conf/httpd.conf	Hourly
/usr/sbin/slapd NTM release is 12.0 or later		-f /nm/web/sup_soft/ldap/conf/slapd.conf	Hourly
oraclenm NTM release is 15.0 or later	One per active Oracle connection	The Oracle server process associated with each active connection.	

Table 1 Monitoring Process (continued)

Process Name	Instances	Comments / Arguments	Intervals
ccintf NTM release is 15.0 or later	One per periodic data type, event analysis (available from release 16.0), and misc. administrative tasks	Primarily used for the thresholding of user defined data types and the insertion of periodic and exception information into the appropriate Oracle table.	
objmgr NTM release is 15.0 or later	One per ccintf process	The table management process associated with each ccintf process.	
Oracle RDBMS processes NTM release is 15.0 or later	Oracle release dependent	This item represents the numerous standard Oracle processes associated with the particular release of the Oracle RDBMS. See the Oracle documentation regarding the naming and task of each process.	

□

19 Training Objectives and Exercises

Overview

Purpose

This Appendix contains objectives and exercises that accompany Alcatel-Lucent Learning course number OS3189.

Objectives

This course prepares students for duties as a system administrator for an NTM system. It is course is designed to enable the student to:

- Add and delete network elements
- Perform general administration tasks, such as managing system security, using administrative commands, and administering and managing databases, adding and deleting users
- Perform printer and backup administration
- Use various utilities for administering the system including links and subnetworks
- Perform NTM computer operations (backup and restore, etc.)
- Administer features of the NTM including; BDR, TCP/IP directly connected network elements, Capacity Usage, and 1024 trunk groups.

Course locations

Courses can be taught at your location. Call 1-614–860–5040 for suitcasing requirements. Enrollment: https://www.lucent-product-training.com, or 1-888-Lucent8 (888-582-3688), prompt 2, prompt 2

□

Chapter 2, “Adding and Removing Users on the Host”

Objectives

This lesson is designed to teach you how to:

- add users to the host
- remove users from the host.

Exercises

1 Which file is updated by the process of adding and removing users?

2 What command is used to remove users: deluser or rmuser?

3 `True or False:` Both the root password and the nmadm password are required to add or remove users.

4 `True or False:` All logins on the system can be removed with the above command.

□

Chapter 3, “System Security, User Groups, and Group Permissions”

Objectives

This lesson is designed to teach you how to:

- determine what user groups are predefined on the system.
- describe the layout of the /etc/permission file.
- add and remove user groups.

Exercises

1 Which of the following is NOT a predefined user group?

- sys
- snm
- srb
- rb
- admin
- usr

2 `True or False:` Since permission are login-based, members of the same group may have different command permissions.

3 `True or False:` The permissions file cannot be edited directly; permissions must be changed using system utilities such as addgroup and adduser.

4 How many groups may be given permission to use a single command?

5 Can a user belong to more than one group?

6 `True or False:` Groups may be added using either the addgroup command or the snw_admin menu.

7 `True or False:` Groups may be removed using either the snw_admin menu or the rmgroup command.

□

Chapter 4, “Starting and Stopping the System”

Objectives

This lesson is designed to teach you how to:

- start the system.
- stop the system.
- halt and boot the system.

Exercises

1 Which command (sysstart or startsys) starts the NTM system?

2 `True or False:` The root password is required to start the system.

3 Which command option (-r or -h) halts the system processes with automatic reboot?

4 `True or False:` Both the root and nmadm passwords are required to halt and boot the system.

□

Chapter 5, “Backing Up and Restoring the System”

Objectives

This lesson is designed to teach you how to:

- perform various types of backups on the system.

Exercises

1 Which RHEL utility is used to schedule automated full and incremental backups?

2 How often should an incremental backup of the user-modifiable files be made?

3 For which of the following backup types must the system be stopped?

- Full/incremental backup of all file
- Backup of the system root disk
- Archive of historical data
- Backup of user-modifiable files

4 How often should the system root disk be backed up?

5 `True or False:` An archive of historical data may be made in the same way as a full or incremental file system backup.

6 Are there files and directories which should be excluded from full and incremental backups?

□

Chapter 5, “Backing Up and Restoring the System”

Objectives

This lesson is designed to teach you how to:

- restore data to the system from backups.

Exercises

1 `True or False:` Full and incremental backups are interchangeable.

2 Can the entire root or /usr file systems be restored from backup tapes?

3 How much historical data does an archive tape contain?

4 `True or False:` The NTM application must be stopped before restoring files from tapes made with the HP-UX SAM utility.

5 `True or False:` The HP-UX SAM utility allows file systems, directories, or individual files to be recovered.

□

Chapter 7, “Administrative Performance Reports”

Objectives

This lesson is designed to teach you how to:

- gather Linux system performance statistics with the Linux tools sar and runacct.
- use the Performance and Troubleshooting Reports (PATR) feature.

Exercises

1 What does the sar package provide?

2 What does the runact package provide?

3 What data is provided by `perfrep`?

4. I want to know what switches are not reporting 5-minute data, or are reporting late. Write the `failrep` command syntax to do this.

□

Chapter 8, "Database Administration"

Objectives

This lesson is designed to teach you how to:

- identify how the disk array is configured
- interpret the logical layout of the disk array
- determine database status
- understand database recovery procedures

Exercises

1 How much disk space is allocated to each historical database?

2 How many historical databases are configured on the system?

3 Which Logical Unit Number (LUN) contains the NM file system?

4 In addition to the historical databases, there are three other databases on the system. What are these databases?

5 What command is used to determine database status?

6 Will the command referred to in Exercise 6 allow you to change the status of a database?

7 Under what circumstances should the database recovery procedures be used?

□

Chapter 11, “Subnetwork Administration”

Objectives

This lesson is designed to teach you how to:

- use Subnetworks.

Exercises

1 Explain the purpose of subnetworks.

2 What is the maximum number of subnetworks that may be defined?

3 What command is used to create a subnetwork?

4 There are two levels of subnetwork permissions. Define them.

5 In which record base file are office subnetwork memberships defined?

6 `True or False:` User group permissions are limited to one subnetwork per user group.

□

Chapter 12, “BDR Administration on a Host”

Objectives

This lesson is designed to teach you how to:

- administer BDR.
- activate BDR.
- deactivate BDR.

- take over operations from a failed host.

Exercises

1 Does reference data for a secondary host exist on the primary host in a: 1) record base partition or 2) a subnetwork?

2 Do the `bdr_act` and `bdr_deact` commands require the root login, the nmadm login, or both?

3 Do `bdr_takeover` and `bdr_switchbk` require the root login, the nmadm login, or both?

Chapter 14, “Capacity and Usage Reporting”

Objectives

This lesson is designed to teach you how to:

- understand what types of Data are collected?
- explain what type of reports you can request?
- interpret reports
- interpret a failrep report

Exercises

1 Name three out of the seven types of data collected.

2 Can you specify what month, day, and times you want a report?

3 How long is data retained?

4 `True or False:` You can run the perfrep command as many times as you want in one day.

5 Under the description Data Access - Demand, what is the maximum or expected value?

6 Under the CPU Usage Data Collection Section - User Interface - Performance, what is the maximum or expected value?

7 What two types of real time reports can be generated with the failrep command?

8 What is an rsp_code?

□

Glossary

%	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	W

%%OCC Percent Occupancy

The fraction of time that a circuit or a piece of equipment is in use, expressed as a decimal. Numerically, it is the Erlangs carried, and it equals the carried CCS divided by 36. Percent occupancy measurements include both message time and setup time.

%OFL Percent Overflow

The relationship between the total attempts offered in a specific time period to a route or a destination and the number of attempts not finding an idle circuit.

AAB A-B trunk group

A trunk group that connects an originating office (A) directly to a terminating office (B). See “AV” (p. 3) and “VB” (p. 25).

ACC Automatic Congestion Control

Senses machine congestion and activates preplanned internal and external overload controls. Also called/see also DOC. See the acc command (4-9) in the *Input Commands Guide*.

ACG

Automatic Call Gap

ACH Attempts per Circuit per Hour

Relationship between the number of attempts that result in an answer signal and the total number of attempts.

ACM Address Complete Message

A messages sent in the backward direction indicating that all the address signals required for routing the call to the called party have been received.

Activate

To make an office active for data collection.

ADL-V

AT&T Digital Link — Phase 5

Aggregated Trunk Group

An aggregated trunk group is not a physical trunk group but rather a collection of all traffic information on trunk groups to a particular "to office”, represented with a unique trunk group ID. In this way, controls can be sent to a 7R/E switch for a given "to office" by specifying the tg ID of the aggregated trunk group.

Aggregation Limit

Date and time limit you can set on the aggregation view to limit the number of records that will appear in your report.

AIC Available Idle Circuits

A traffic measurement used by network managers to determine which trunk groups have capacity available for rerouting traffic from an overloaded trunk group.

AIN Advanced Intelligent Network Also called an Intelligent Network) A network:

- That affects the routing of calls within it from moment to moment based on a criteria other than simply finding a path through the network for the call
- Where the originator or the ultimate receiver of the call can inject intelligence into the network and affect the flow of his call (either outbound or inbound).

Intelligent networks generally include SCP, SSP, and STP components.

Alarm

Visible report of a trouble condition in the network. Alarms usually require immediate attention from network personnel.

Alert

Visible report of a potential trouble condition in the network.

Alerting Discrete

An on/off indicator that notifies network managers of changes to the status of the office. An alerting discrete provides a message to NTM that starts a corresponding audit (unless that audit has been previously inhibited by the network manager).

Allow

Indicates the permitting of an action, such as permitting automatically triggered audits to run.

Alternate Routed Traffic

Traffic that has been offered to a previous trunk group and has not been able to find an idle circuit. The switching system handling the traffic then offers it to an “Alternate Route,” based on its internal routing tables.

Alternate Routing

A means of selectively distributing traffic over a number of routes, ultimately leading to the same destination.

APC

Adjacent Point Code

APR Allow Previously Rerouted

A trunk group reroute control option that allows previously rerouted traffic to reroute. Only *4ESS* and *5ESS* offices support this reroute control option.

APS

Attached Processor System

ASCII American Standard Code for Information Interchange

A 7-bit code for providing as many as 128 different characters. An eighth bit can be added as a parity check for error detection purposes.

ASP

Advanced Services Platform

ATM Asynchronous Transfer Mode

A high bandwidth, low-delay, connection-oriented, packet-like switching and multiplexing technique that allows very high speed transmission.

Attempt

An attempt to seize a circuit in a route. An attempt may be successful or unsuccessful.

Audit

An integrity check through which NTM corrects differences between its own database and office databases.

AV

A-V (via) trunk groups. A trunk group that connects an originating office (A) to a via office (V). See “AB” (p. 1) and “VB” (p. 25).

BBacking Up

The process of copying data onto a separate medium for the purpose of data retention.

BDR Backup and Disaster Recovery

See Feature 8, “Disaster Recovery (Duplex)” and Feature 40, “Enhanced Disaster Recovery” in the *System Overview*.

Blocking

The inability of the calling party to be connected to the called party because either all suitable trunk paths are busy or a path between a given inlet and any suitable free outlet of the switching network is unavailable.

Broadcast Message

A text message sent out by personnel using the NTM to other users on the system.

CCalculation

Calculated counts used to signify changing network conditions and, when thresholded, to alert network managers to events that might require action to prevent excessive network congestion.

CAMA Centralized Automatic Message Accounting

Specific version of AMA in which the ticketing of toll calls is done automatically at a central location for several central offices.

CANF Cancel From

A post-hunt protective trunk group control that prevents a percentage of overflow traffic for a selected originating trunk group from advancing to any alternate route. See the canf/cant/skip command (4-13) in the *Input Commands Guide*.

CANT Cancel To

A pre-hunt protective trunk group control that prevents a percentage of traffic from accessing a selected destination trunk group. See the canf/cant/skip command (4-13) in the *Input Commands Guide*.

CCIS Common Channel Interoffice Signaling

Carries telephone signaling information along a path different from the path used to carry voice.

CCITT

Consultative Committee on International Telegraphy and Telephony

CCS Centi (Hundred) Call Seconds

A unit of traffic used to express the average number of calls or the average number of devices in use. One CCS is equal to the continuous load for 100 seconds. The CCS for an hour is 36.

CCS Common Channel Signaling

A form of signaling in which a group of circuits share a signaling channel.

CCS7-NA

North American Version of CCITT#7

CG Call Gap

A protective control that allows a fixed number of calls to succeed to a code (telephone number) in a 5-minute interval. See the cg command (4-21) in the *Input Commands Guide*.

CGX

Call Gaps with an IC prefix (*1AESS* only)

CICR Cancel In-Chain Return

A reroute trunk group control option. When set to YES, does not allow traffic to return to in-chain routing. When set to NO, allows traffic to return to in-chain routing.

CLI

Caller Line Identification

Client

A client uses the resources of another device (computer) or application. Client is another term for a PC on a local area network.

CLLI

Common Language Location Identifier

CNI

Common Network Interface

Code

A numbering system for telephone addresses, for example, 614-555-1234 (NPA-NXX-XXX).

Connection

An attempt for a circuit that succeeds in obtaining a circuit. Also called a seizure.

Container Page

One of the five basic types of pages used in the GUI. It displays the results of a search or a map of a network area.

Control Data
Data that describes the actual controls in place for the network.

CPE
Customer Premises Equipment

CPU
Central Processing Unit

CR
Critical Alarm

CR Circuit Reservation
An automatic trunk group control that reserves the last few trunks of a trunk group for critical users exclusively and eliminates the need to queue critical users for inter-switch trunks. See also/also called STR. See the cr command (4-32) in the *Input Commands Guide*.

Crash Dump
The output from the hardware registers, the hardware stack, and the CPU.

CRO Cancel Rerouted Overflow
A reroute trunk group control option that prevents overflow traffic on a via route (VB) from overflowing back to the direct route (AV). Not activating the CRO can result in an external loop.

CSL
Communications Software Launcher

Customer Premises Equipment
All telecommunications terminal equipment located on the customer premises.

DDatabase
A collection of data organized for rapid search and retrieval by a computer.

DCC
Data Collection Concentrator

DCE
Distributed Computing Environment

DCS
Display Construction Set

Deactivate
To make an office inactive for data collection.

Demand Data

Data retrieved by the demand command (5-21) from the system database. The User Report Writer feature and SQL files use this data to create informational reports.

Destination

A specified area or country in which the called subscriber is located. A destination is identified by its destination code (the digits used for routing the call).

Detail Page

One of the five basic types of pages used in the GUI. It provides information (such as reference data) on specific network elements or network connections.

Direct Routed Traffic

Traffic that is being offered to the trunk group for the first time, not having been previously offered to a different trunk group. This traffic, which has not alternate routed, is sometimes called “First Routed” traffic.

Discrete

An on/off indicator that notifies network managers that:

- Changes have been made to the status of the office
- Significant events have taken place within the office

NTM polls the offices for discretes at regular intervals.

Disk Array

A disk subsystem combined with management software that controls the operation of the physical disks and presents them as one or more virtual disks to the host computer.

DOC Dynamic Overload Control

Also called/see also ACC

Domain

A type of calling service, such as POTS (Plain Old Telephone Service), ACNT (*Accunet*), SDN (Software Defined Network), or ISDN (Integrated Services Digital Network).

Dot Profile (.profile)

A file located in your home directory that alters your default *Linux* system environment. You can use your .profile to define environmental variables such as your terminal type, prompt string, or mailbox address.

DP

Dial Pulse

DPT

Dynamic Packet Trunks

DPTPRI
Dynamic Packet Trunks Prioritization

DPTRES
Dynamic Packet Trunks Reservation

DPTTID
Dynamic Packet Trunks Terminal Identifier

DSC
Dynamic Service Control

DSDC Direct Services Dialing Capability
Network services provided by local switches interacting with remote databases via CCIS.

DTMF
Dial Tone Multifrequency

DTS
Dial Tone Speed

EEA Equal Access
A trunk group reroute option for switches that limits the reroute to equal access traffic.

EADAS Engineering and Administration Data Acquisition System
A system in which traffic data are measured at switching systems by electronic devices, transmitted to a centrally located minicomputer, and recorded on magnetic tape in a format that is suitable for computer processing and analysis. Performs data collection in NTM for certain switch types.

Erlang
A measurement of traffic load equal to the continuous occupancy of one circuit (or unit of equipment) for one hour. An Erlang can express the capacity of a system; for example, a trunk group of 30 trunks, which in a theoretical peak sense might carry 30 Erlangs of traffic, would have a typical capacity of perhaps 25 Erlangs averaged over an hour.

Error Code
An identification field used to identify the module or feature reporting the error. See the **ERR_CODE** field help file.

Error Log
The error log is a file that contains the error messages being generated by NTM. See the errlog command (9-7) in the *Input Commands Guide*.

Error Messages

System responses resulting from software-detected errors, changes in the system status, or non-executable commands.

Error Number

Number associated with error codes that help identify specific messages. See the **ERR_NUM** field help file.

ESP

Essential Service Protection Triggered

ESS

Electronic Switching System

ETR Easy To Reach

A code (telephone number) is determined to be easy to reach because the attempts and failures to the code do not exceed user-defined thresholds.

Exception

A calculation based on office or trunk group data that exceeds a user-defined threshold. It indicates an abnormal working condition in the network.

Exception Level

A number associated with an exception, indicating the severity or priority of the exception. High-numbered exception levels are more severe.

Exception Processing

Process used to collect raw data from the switch, perform calculations on the data, and, as a result, find exceptions based on predefined thresholds.

Exception Report

Formatted report of all exceptions that have occurred during the most recent 5-minute period.

Execution Error

The NTM GUI presents error messages in response to conditions such as improper permission, execution errors, etc. Execution errors are related to the execution of requests that affect the network elements to which the NTM host is connected (e.g., control requests or HTR administration).

External Network Element

A network element that is defined in the NTM Record Base but for which surveillance data is not received by NTM.

FFEP Front-End Processor

An application that acts as a DCC. Available with purchase of Feature 214, “FEP Release 4” or Feature 257, “FEP Release 5”.

FHC

Final Handling Code

Final Trunk Groups

A trunk group that acts as a final route for traffic. Traffic can overflow to a final group from high-usage groups that are busy. Traffic cannot overflow from a final trunk group. Calls that overflow a Final Trunk Group are terminated unless they are rerouted by an NTM Reroute control. See the rr command (4-44) in the *Input Commands Guide*.

FML Field Manipulation Language

A set of C-language functions for defining and manipulating data storage structures called fielded buffers.

FOO

A foo is a term universally substituted for something real when discussing ideas or presenting examples.

From Office

Internal network element that originates the trunk group.

FSD

Feature Specification Document

Full Create

The process of constructing the database itself (once the database files have been prepared) or making major database modifications through the use of the `create` command with no arguments. This process also modifies the offline database.

Full Trunk Group

A trunk group that does not overflow calls to another trunk group because enough trunks are provided to give an acceptable blocking probability.

GGeneric

The version released to provide specific services, features, or functions.

GETS

Government Emergency Telecommunications Service

GSC

Group Signaling Congestion

GSM

Global Switching Module

GUI Form Elements

The elements that appear within a form on a web page. Form elements may consist of a label and one or more fields when they are used outside a table. See "GUI form elements" (p. 20) in the *User Guide*.

Hhecto

A unit of measure meaning 10 to the power of 2.

High-Usage Trunk Group (HU)

A trunk group that is the primary direct route between two switching systems. The group is designed for high average occupancy. To provide an overall acceptable probability of blocking, an alternate route must be provided for overflow traffic.

Host Computer

Computer (machine) used to run the NTM.

HPC High Probability of Completion

A phase of GETS that extends the enhanced routing and priority service to LEC networks traversed by the call.

HT Holding Time

The average duration of phone calls.

HTR Hard-To-Reach

A code (telephone number) is designated as hard-to-reach because the number of attempts and failures to the code exceed user-defined thresholds. See Chapter 7, "Hard-To-Reach (HTR)" in the *System Overview*.

HU High Usage

A trunk group that is the primary direct route between two switching systems. The group is designed for high average occupancy. For an overall acceptable probability of blocking, an alternate route must be provided for overflow traffic.

Hunt Types

The three hunt types for reroutes are ***regular***, ***order***, and ***spray***.

- The regular hunt uses only one out-of-chain engineering route for the reroute. Order and spray hunts can have from two to seven out-of-chain engineering reroutes.

- For the order hunt, an ordinary route-advance pattern is specified for the out-of-chain engineering reroutes, and the same route is always used as the starting point for the trunk hunt.
- For the spray hunt, rerouted traffic is divided evenly among the out-of-chain engineering routes through a rotation scheme.

See the HUNT field help file.

Hysteresis
The minimum amount of change required to make a difference.

IICCH Incoming Connections per Circuit per Hour
The incoming peg count divided by the number of equivalent 2-way circuits.

IEC
InterExchange Carrier

IMA
Ineffective Machine Attempts

Immediate Reroute
A reroute that diverts calls to one or more specified via trunk groups prior to the hunting of the "reroute from" trunk group.

IMS
IP (Internet Protocol) Multimedia Subsystem

INA
Ineffective Network Attempts

Incoming Calls
Incoming trunk seizures at the office.

Inhibit
Indicates the blocking of an action, such as blocking automatically triggered audits from running.

Input Command
User-invoked instructions to a system, entered in the command shell. Also called an input message and command. See the *Input Commands Guide*.

Internal Calls
Originating calls intended to complete on lines served by the switch.

Internal Error Message
An error message reported in the error log and on the system console.

Internal Network Element
Network elements from which surveillance data is collected.

INWATS Inward Wide Area Telephone Service
A service that allows subscribers to receive calls from specified areas with no charge to the person who's calling.

IP
In Progress

IRR Immediate Reroute
A pre-hunt trunk group control option that causes a percentage of a specified type of traffic to be rerouted before it is offered to the regular in-chain trunk group.

ISA
Integrated Service Assurance

ISDN Integrated Service Digital Network
A set of standards for digital transmission over ordinary telephone copper wire as well as over other media. ISDN integrates analog or voice data together with digital data over the same network.

Issue
Office generic issue number.

ISUP Integrated Service Digital Network User Part
Defines the protocol and procedures used to set up, manage, and release trunk circuits that carry voice and data calls over the public switched telephone network (PSTN). ISUP is used for both ISDN and non-ISDN calls. Calls that originate and terminate at the same switch do not use ISUP signaling.

IWBM
Inter-working Bridge Measurements.

LLATA
Local Access and Transport Area

Launch page
One of the five basic types of pages used in the GUI. It is used to select high-level data types to monitor.

LEC
Local Exchange Carrier

Link Status
The signaling system connection status of an office.

LNP
Local Number Portability

Logical Database
A logical database consists of a computer program system database and a *Linux* operating system file area.

LRN
Location Routing Number

LSSGR
LATA Switching System Generic Requirements

MMB Maintenance Busy
Conditioning a circuit, a terminal, or a termination to be unavailable for service. When unavailable, it is generally necessary that it appear busy to circuits that seek to connect to it. Sometimes referred to as “make busy”. See the MB field help file.

MC
Machine Congestion Level

Menu Mouse Button
Mouse button used to display context-sensitive menus. (Usually the right mouse button.) Click the menu mouse button once to display the menu, then use the Select Mouse Button to select an item (or subitem) from the menu.

MF
Multifrequency

Mnemonic
Executable name used to access menus, menu items, and pages on the terminal screen. A mnemonic is a word or string that is intended to be easier to remember than the thing it stands for.

Monitoring
Comparing the traffic on selected trunk groups with assigned thresholds.

MSU
Message Signaling Unit

MTP Message Transfer Part

The part of the SS7 protocol that provides for basic routing of signaling messages between signaling points.

NNC

No Circuits

NCP Network Control Point

A routing, billing, and call control database system.

NEA Non-Equal Access

A trunk group reroute control option for switches that limits the reroute to non-equal access traffic.

Network Traffic Management

A system that provides near-real time surveillance of the network elements connected to it for the purpose of managing network congestion.

Network Data

Traffic data that is collected from the network elements on a periodic basis, typically 5 or 15 minutes.

Network Management

A set of procedures, equipment, and operations designed to keep a traffic network (a telephone network, for example) operating near maximum efficiency when unusual loads or equipment failures would otherwise force the network into a congested, inefficient state.

Network Management Data

A combination of data collected from the switches and data entered in the record base. This data describes the base of the network and what occurs in the network.

NFS Network File System

A distributed-file-system protocol that allows a computer on a network to use the files and peripherals of another networked computer as if they were local.

NHR Not Hard-to-Reach

A code (telephone number) determined to be not hard-to-reach because the attempts and failures to the code do not exceed user-defined thresholds.

NMC Network Management Center

A centralized location at the network management layer used to consolidate input from various network elements to monitor, control, and manage the state of a network in a telecommunications organization.

NOCS Network Operation Center

A group responsible for the day-to-day care of a network.

NPA Numbering Plan Area

A geographic division within which telephone directory numbers are subgrouped. A 3-digit NXX (local office) code is assigned to each NPA, where:

- N=any digit 2 through 9
- X = any digit 0 through 9

NPR

NTM Performance Reporting

NS

Number Service

NTM

Network Traffic Management

NTM **Host**

The server on which the NTM is run.

OOCC Occupancy

The time a circuit or switch is in use.

OCCH Outgoing Connections per Circuit per Hour

The outgoing peg count divided by the number of equivalent 2-way circuits.

Office

A local switch, DCC, or FEP connected to your host computer.

OFL Overflow

Number of attempts failing to find an idle circuit in a group of circuits.

One-Way Trunk

A trunk that can be seized at only one end.

Ongoing Data

Data retrieved by the `ongoing` command from the system's shared memory.

Originating Calls

Line seizures at the office.

ORR Overflow Reroute

A reroute post-hunt trunk group control option that takes the overflow traffic on a trunk group and reroutes it to a trunk group with idle capacity.

Outgoing Calls

Calls intended to complete on trunks to points outside the system (same as outgoing seizures).

Overflow Peg Count

Peg count overflowing to another trunk group or to a circuit busy signal.

OVLD Overload

An increase in offered load beyond the capacity for which the network components (for example, trunks and switching systems) are engineered.

P

Page

A page is a universal resource locator (URL), part of the NTM application. A page is displayed inside a Window. The user selects, changes and transfers pages within the same window.

Parameter area

The area of a control request display that contains various control parameters.

Parameter Set

A predefined group of control parameter values that may be used to quickly apply a control to one or more switches.

PAS

Public Announcement Service

PATR   Performance and Troubleshooting Reports

This feature enables NTM personnel to collect various office and application performance data, and to output reports on request. Depending on the report type selected, the data may be real-time or hourly. The hourly data may be for a 24-hour period or less. Seven days of data are collected and stored for report access.

PC Peg Count

A count of all calls offered to a subgroup during a measurement interval.

PCI

Panel Call Indicator

PIIT Prohibit International Inbound Traffic

A reroute trunk group control option. When set to YES, does not allow inbound international traffic to be rerouted. When set to NO, allows inbound international traffic to be rerouted. See the rr command (4-44) in the *Input Commands Guide*.

Post-Hunt Control

A trunk group control that may affect a call that is attempting to alternate route to the next designated trunk group, for example: CANF.

PP

Preprogram

PPC

Peripheral Processor Complex

Pre-Hunt Control

A trunk group control that may affect a call before it is offered to a particular trunk group, for example: CANT, SKIP.

Preplan

Command used to create and manage pre-designated control plans to be used in emergency situations. See the preplan command (4-72) in the *Input Commands Guide*.

PS/UT

Pseudo-Subunit / Unit Type

PTS

Public Telecommunications Systems

QQOR

Query on Release

RRADR

Receiver Attachment Delay Readiness

RC

Routing Code

RDB

Routing Data Block

Real Time Usage

The percentage of time used out of total available real time, not including multi-task time.

Record Base

A collection of ASCII files containing reference information about the network to be managed by NTM.

Record Base Administration
The process of creating and maintaining the reference data portion of the NTM database.

Reference Data
Data that describes what the network is managing. This consists of either data about the network management center itself (such as the configuration of the center and threshold tables) or data about the network being monitored (such as the switching systems and trunk groups in the network management center's cluster). User-defined reference data is stored in the “/musr/rb” directory. Some reference data is supplied to the database by audits. This data typically changes infrequently.

Regular Expressions
A way of searching for patterns of characters in text strings. In NTM, it applies to Network Element search fields used to find particular switches or trunk groups.

Reorder Tone
A tone that is applied 120 times per minute to indicate all switching paths busy, all toll trunks busy, equipment blockages, unassigned code dialed, or incomplete registration of digits at a tandem or a toll office. Also called **Channel Busy** or **Fast Busy Tone**.

Request Page
One of the five basic types of pages used in the GUI. It is used to display control parameters before a control is applied.

Reroute
See “RR” (p. 20).

Reservation Level
The Circuit Reservation (CR) control allows the user to specify a maximum number of idle circuits to reserve and what the switch is to do with direct and/or alternate routed traffic when the reservation level is reached.

RLU
Remote Line Unit

ROA
Re-Order Announcement

Route
One or more trunk groups providing a connection between offices.

Route Group
A route group consists of one or more routes that may be used for a given destination. A route group may be accessed by more than one combination of destination and additional parameters.

RP Revertive Pulse

Revertive Pulsing is a method of signaling between switching systems in which information is conveyed from System A to System B. System B sends a sequence of pulses to System A, where the pulses are counted. System A signals System B when the correct number of pulses has been received.

RR ReRoute

An expansive trunk group control that is used to take traffic from congested or failed routes to other trunk groups not normally included in the route advance chain. These other trunk groups, called “vias,” should have available idle circuits (AIC) to be used for the reroute. See the rr command (4-44) in the *Input Commands Guide*.

RSPTE Regional, Sectional, Primary, Toll, and End office

See the “RSPTE File” (p. 68) in the *Record Base Administration Guide*.

RSU

Remote Switching Unit

SSCCP Signaling Connection Control Part

A signaling protocol that provides additional routing and management functions for transfer of messages other than call setup between signaling points.

SCP Service Control Point

A remote database within the SS7 network that supplies the translation and routing data needed to deliver advanced network services. Also called Signal Control Point.

SDM

Supernode Data Manager

SDN Software Defined Network

A service developed for multi-location businesses that allows network managers to tailor their network to their own specific communications needs.

SDOC

Selective Dynamic Congestion Control/Automatic Congestion Control

Search Page

One of the five basic types of pages used in the GUI. It is used to request data on network elements, network connections, and controls. It can be used in simple or advanced modes.

Seizure

An attempt for a circuit in a trunk group that succeeds in obtaining a circuit.

Select Mouse Button

Mouse button used to specify an object to operate on and to manipulate objects and controls. (Usually the left mouse button.)

Set

Logical grouping of network elements (offices or trunk groups). NTM with standard features allows each office to be a member of up to four office sets, and each trunk group to be a member of up to four trunk group sets.

Shared Memory

A RAM-based data structure on the host that is used to store discrete, control, and exception data. Portion of memory accessible to multiple processes.

Signaling

The transmission of address (pulsing), supervision, or other switching information (including any information required for billing) between stations and switching systems, and between switching systems.

SILC Selective Incoming Load Control

An automatic trunk group control that can be enabled or disabled on a selected trunk group in a “From Office” when the office encounters machine congestion. See the silc command (4-55) in the *Input Commands Guide*.

Single File Create

The process for creating (compiling) individual record base files.

Single Office Create

The process for creating (compiling) all office-related files for one office only. A single office `create` acts directly on the current database; no `installdb` command is necessary to install the changes to the database. See the *Record Base Administration Guide*.

SKIP Skip route control

A pre-hunt trunk group control that allows all or a percentage of traffic to bypass a specific route and to advance to the next route in its normal routing pattern. See the canf/cant/skip command (4-13) in the *Input Commands Guide*.

SMS Service Management System

Allows provision and updating of information on subscribers and services in near-real time for billing and administrative purposes.

SQL Structured Query Language

Database language used for creating, maintaining, and viewing database data. See Chapter 3, “SQL Interpreter” in the *Data Tables Guide*.

SQL File
A data request file that lets you specify what data should be retrieved from the database or the ongoing shared memory and to define the format of the data.

SS7 Signaling System 7
Signaling protocol that uses destination routing, octet-oriented fields, variable length messages and a maximum message length allowing for 256 bytes of data. The four basic sub-protocols of SS7 are: MTP, SCCP, ISUP, and TCAP.

SSP Service Switching Point
A switch that can recognize IN (Intelligent Network) calls and route and connect them under the direction of an SCP. Also called **Signal Switching Point**.

STP   Signal Transfer Point
A message switching system that permits signaling messages to be sent from one switching system to another by way of one or more other offices at which STPs are located. It reduces the number of data links required to serve a network.

STR Selective Trunk Reservation
An automatic trunk group control that reserves the last few trunks of a trunk group for critical users exclusively and eliminates the need to queue critical users for inter-switch trunks. Also called CR/TSR. See the cr command (4-32) in the *Input Commands Guide*.

Subnetwork
A subdivision of the network that allows parts of the network to be monitored and controlled independently of the main network.

Suffix
A user-defined string (up to 5 characters long) used to identify a particular office or trunk group. The suffix is separated from the office or trunk-group name by a hyphen.

Surveillance Data
Discrete and measurement data collected periodically from the switch.

SVC   Switched Virtual Circuit
A virtual circuit connection established across a network on an as-needed basis and lasting only for the duration of the transfer.

Switch
A computer system that channels telephone calls from one place to another and keeps track of each call that it transfers.

Switch Name
A code name that identifies an office.

Syntax

The format in which a command is entered, including the input command name, parameters, and action options.

System Error

The NTM GUI presents error messages in response to conditions such as improper permission, execution errors, etc. A system error is presented when an error occurs on the NTM host during the generation of a web page or during the processing of a request from a web page (except certain control related requests).

TTandem Office

In general, an intermediate switching system for interconnecting local and toll offices. All toll offices are tandem offices. A more specific meaning of local tandem or metropolitan tandem office is an office that connects end offices to other end offices or to other tandem offices within a metropolitan area.

TCAP Transaction Capabilities Application Part

A signaling protocol that provides for transfer of non-circuit related information between signaling points.

TCU

Time Switch and Peripheral Control Unit

TDM

Time Division Multiplexing

Terminating Calls

Calls intended to complete on lines served by the system.

TFP

Transfer Prohibit

TG Trunk Group

A group of trunks with similar electrical characteristics that go between two geographical points. A trunk group performs the same function as a single trunk, except that on a trunk group multiple conversations can be carried. Trunk groups are used as traffic demands them.

Threshold

A preset limit of exceptions that each network element must exceed during each 5-minute period before NTM determines that the office is experiencing patternable trouble.

Thresholding

The process of setting values to be compared against data values (raw counts) collected from the switches every 5 minutes to determine exception conditions.

TID

Terminal Identifier

To Office

Internal or external network element that is the termination of a trunk group.

TPC

Telephony Processor Complex

Traffic Network

An arrangement of channels, such as loops and trunks, associated switching arrangements, and station equipment designed to handle a specific body of traffic; a subset of the facility network.

Trunk

A telephone communication path or channel between two points, one of them usually being a telephone company central office or switching center.

Trunk Group

See “TG” (p. 23).

Trunk Group Number

Number assigned to a trunk group in the switch.

TSG

Trunk Subgroup

TTO

Transmitter Time-Out

Two-Way Trunk

A trunk that can be seized at either end.

UUDTS

Unitdata Services

URW User Report Writer

The User Report Writer consists of the transaction processing system report writer software package and a system command set. The transaction processing system generates informational reports based on data that changes periodically.

Usage

A measure of trunk or equipment occupancy expressed in Erlangs or CCS.

V

Vacant Code

An unassigned numbering plan area, central office, or station code. A call placed to a vacant code is normally directed to a VCA (vacant code announcement).

Validate

A command used to verify that the values and actions specified are correct for a specific display or page.

VB

V-B (terminating) trunk group. A trunk group that connects a via office (V) to a terminating office (B). See "AB" (p. 1) and "AV" (p. 3).

Via Office

An office that transits a rerouted call between the originating office and the terminating office.

Via Trunk Group

A trunk group designated to carry the calls redirected by a reroute control activated on the "reroute from" trunk group of the reroute control. If a trunk group is identified as a "via trunk group" it is the "AV" portion of the "AV"-"VB" path for rerouted calls.

VRTO Via Route Turnoff Override

VRT is a reroute option that protects regular traffic from rerouted traffic, by not allowing rerouted traffic to use a via TG that is filling with regular traffic. VRTO overrides the VRT option so that network managers can use the via trunk group anyway. See the rr command (4-44) in the *Input Commands Guide*.

W

Window

A window is box-type graphic displayed when specific buttons, icons, function keys or hot keys are selected in a windows operating system environment. Each window contains various control attributes including a means to close the box, typically an "X" in the upper right corner. The window identifier is displayed in the task bar. The user opens and closes windows.

Index