VERSION 3.5

Access

Control

BorderManager™

ENTERPRISE EDITION 3

Novell®

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

The Harvest software was developed by the Internet Research Task Force Research Group on Resource Discovery (IRTF-RD):

Mic Bowman of Transarc Corporation.
Peter Danzig of the University of Southern California.
Darren R. Hardy of the University of Colorado at Boulder.
Udi Manber of the University of Arizona.
Michael F. Schwartz of the University of Colorado at Boulder.
Duane Wessels of the University of Colorado at Boulder.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Access Control
June 1999

TERMS OF USE

The Harvest software may be used and redistributed without charge, provided that the software origin and research team are cited in any use of the system. Most commonly, this is accomplished by including a link to the Harvest Home Page (http://harvest.cs.colorado.edu/) from the query page of any Broker you deploy, as well as in the query result pages. These links are generated automatically by the standard Broker software distribution.

The Harvest software is provided "as is," without express or implied warranty, and with no support nor obligation to assist in its use, correction, modification or enhancement. We assume no liability with respect to the infringement of copyrights, trade secrets, or any patents, and are not responsible for consequential damages. Proper use of the Harvest software is entirely the responsibility of the user.

DERIVATIVE WORKS

Users may make derivative works from the Harvest software, subject to the following constraints:

— You must include the above copyright notice and these accompanying paragraphs in all forms of derivative works, and any documentation and other materials related to such distribution and use must acknowledge that the software was developed at the above institutions.

— You must notify IRTF-RD regarding your distribution of the derivative work.

— You must clearly notify users that you are distributing a modified version and not the original Harvest software.

— Any derivative product is also subject to these copyright and use restrictions.

Note that the Harvest software is NOT in the public domain. We retain copyright, as specified above.

HISTORY OF FREE SOFTWARE STATUS

Originally we required sites to license the software in cases in which they were going to build commercial products/services around Harvest. In June 1995, we changed this policy. We now allow people to use the core Harvest software (the code found in the Harvest "src/" directory) for free. We made this change in the interest of encouraging the widest possible deployment of the technology. The Harvest software is really a reference implementation of a set of protocols and formats, some of which we intend to standardize. We encourage commercial reimplementation of code complying to this set of standards.

export notice

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

LANalyzer, LAN WorkPlace, Novell, and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. BorderManager, Client 32, ConsoleOne, Internetwork Packet Exchange, IPX, NASI, NCP, NDPS, NDS, NetWare 5, NetWare Asynchronous Services Interface, NetWare Connect, NetWare Core Protocol, NetWare/IP, NetWare Link Services Protocol, NetWare Loadable Module, NetWare MultiProtocol Router, NLM, NLSP, Novell BorderManager, Novell BorderManager FastCache, Novell Client, Novell Distributed Print Services, Virtual Loadable Module, VLM, and Z.E.N.works are trademarks of Novell, Inc.

AppleTalk is a registered trademark of Apple Computer, Inc.

Btrieve is a registered trademark of Pervasive Software, Inc.

Cyber Patrol is a registered trademark of Learning Company Properties, Inc.

CyberNOT is a trademark of Learning Company Properties, Inc.

CyberNOT List is a trademark of Learning Company Properties, Inc.

CyberNOT is a trademark of Learning Company Properties, Inc.

CyberYES List is a trademark of Learning Company Properties, Inc.

Hayes is a registered trademark of Hayes Microcomputer Products, Inc.

Java is a trademark of Sun Microsystems, Inc. in the United States and other countries.

JavaScript is a trademark of Sun Microsystems, Inc.

Macintosh is a registered trademark of Apple Computer, Inc.

Microsoft is a registered trademark of Microsoft Corporation.

NCSA is a registered trademark of Bales, Gates & Associates, Inc.

Netscape is a registered trademark of Netscape Communications Corporation.

Netscape Communicator is a registered trademark of Netscape Communications Corporation.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

OS/2 is a registered trademark of International Business Machines Corporation.

PS/2 is a registered trademark of International Business Machines Corporation.

Pentium is a registered trademark of Intel Corporation.

RealAudio is a registered trademark of RealNetworks, Inc.

RealPlayer is a registered trademark of RealNetworks, Inc.

RealVideo is a registered trademark of RealNetworks, Inc.

The Learning Company is a registered trademark of Learning Company Properties, Inc.

UNIX is a registered trademark of X/Open Company, Ltd.

Contents

About This Guide

1 Managing Access Control

Viewing User Statistics 1
Viewing Host Statistics 4
Exporting Data 6
Exporting Data from the Access Control Users Statistics Window 6
Exporting Data Using the Export Logs Option. 8

About This Guide

Novell® BorderManager™ Enterprise Edition 3.5 Installation and Setup provides the basic information you need to set up access control rules.

This documentation provides the following additional information: Chapter 1, “Managing Access Control,” on page 1—Describes how to manage the access control log file.

chapter

1 Managing Access Control

This chapter explains the tasks you must complete to manage Novell® BorderManager™ access control by checking the access control log. It contains the following sections:

- "Viewing User Statistics" on page 1
- "Viewing Host Statistics" on page 4
- "Exporting Data" on page 6

Viewing User Statistics

To display the User Statistics window, complete the following steps:

1. **In NetWare® Administrator, click the Server object representing the BorderManager™ server.**

2. **Select Novell BorderManager from the Tools menu.**

3. **Select View Access Control Log from the BorderManager menu.**

   The Access Control Users Statistics window has two list boxes: the Number of Users list box and the Hosts Accessed by User list box. Initially, the list boxes are empty.

4. **To display the records for a set of connections from a specific user to a specific host, select Display Records and enter a time range for the records you want displayed.**

   For a U.S. English system, the dates are entered in the order of month, day, and year. The order is year, month, and day for a Japanese system; and day, month, and year for European language systems.

   While the records are being read, a dialog box displays the number of records processed, the date and time of the last record that was read, and

a status bar showing the portion of the records read based on the range of dates specified. Cancel the query process at any time by clicking Cancel. Records that have been read are displayed in the Access Control Users Statistics window.

Note You can click the column heading of either list box to sort the entries in that column in ascending or descending order. The sorting order is reversed each time you click the column heading.

The Number of Users list box provides the following information about activity through access control:

- Username— NDS™ name or IP address of the user. In the case of an IP address, the Domain Name System (DNS) domain name will be displayed if it exists in the local DNS list. The local DNS list is built each time the command WHO IS or DNS Hostname is invoked using the right-click menu.
- Hosts Accessed—Number of hosts accessed for the specified period of time.
- Connections—Total number of connections used to access hosts.

The Hosts Accessed by User list box provides the following information about activity through access control:

- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS name or IP address of the accessed host.
- Allowed—Total number of connections granted access to the host for a user.
- Denied—Total number of connections denied access to the host for a user.

5. To display additional types of user information, do the following:

5a. To display all the connections made by a user, double-click a username in the Number of Users list box.

The Access Control Log window displays the following information about the user's activity through access control:

- Entry Time—Time connection was established.
- Username—NDS name or IP address of user.

- Access—Action specified in the access rule for this connection.
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS name or IP address of the accessed host.
- Service—Service used to access the host: Proxy Services or Novell IP Gateway.
- Rule Number—ID number of the rule that grants or denies access to hosts.

5b. To see a description of the rule for a connection between a user and a host, double-click the connection entry in the Access Control Log window.

The Rule Description window provides the following information about activity through access control:

- Rule Number—ID number of the rule that grants or denies access to hosts.
- Date of Creation—Day and time the rule was created.
- Action—Whether the connection is allowed or denied.
- Source—IP address, hostname, or interface name of the connection source to which the rule is applied.
- Destination—IP address, hostname, or interface name of the connection destination to which the rule is applied.
- Access Specification—Any protocol, URL, or Cyber Patrol* rule that determines connection access or denial.

5c. To view usage trend graphs, click Usage Trends in the User Statistics window, then select any of the following graphs to view usage trend data by time of day in one-hour increments:

- Users—Bar graph showing the number of unique users allowed to connect to a host.
- Hosts Accessed—Bar graph showing the number of hosts accessed.

- Access Volume—Line graph showing the number of allowed and denied connections.
- Access Allowed—Bar graph showing the number of allowed connections.
- Access Denied—Bar graph showing the number of denied connections.
- Users, Hosts, and Access Volume—Combination line and bar graph showing the number of users, hosts accessed, and total connections.

All graphs can be saved to disk, copied to the clipboard, or printed.

Viewing Host Statistics

To display specific host information, complete the following steps:

1. **In NetWare® Administrator, click the Server object representing the BorderManager™ server.**

2. **Select Novell BorderManager from the Tools menu.**

3. **Select View Access Control Log from the BorderManager menu.**

4. **To display the records for a set of connections from a specific user to a specific host, select Display Records and enter a time range for the records you want displayed.**

5. **To see which users have accessed a host, double-click the entry for that host in the Hosts Accessed by User list box in the User Statistics window.**

   The Access Control Hosts window displays two list boxes: the Number of Hosts list box and the User Access list box. As in the User Statistics window, the entries can be sorted by selecting the column headings.

   The Number of Hosts list box provides the following information:

   - Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
   - Hostname—DNS name or IP address of a host.

- Users Accessed—Number of users who have accessed the selected host.
- Connections—Number of connections that have been allowed access.

The User Access list box provides the following information:

- Username—IP address or DNS name of the user who accessed the host.
- Allowed—Number of connections granted access to the host.
- Denied—Number of connections denied access to the host.

6. **To see a list of connections for users who have accessed a host, double-click the entry for the host in the Host Statistics window.**

   The Access Control Log window for the selected host is displayed. The Rules Description window can be viewed by double-clicking an entry.

   The Access Control Log list box provides the following information about activity for the selected host through access control:

   - Entry Time—Time connection was established.
   - Username—NDS name or IP address of the user.
   - Access—Action specified in the access rule for this connection: either Allowed or Denied.
   - Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
   - Hostname—DNS domain name or IP address of the accessed host.
   - Service—Service used to access the host: Proxy Services or Novell IP Gateway.
   - Rule Number—ID number of the rule that grants or denies access to the hosts.

Exporting Data

The access control log is stored in a Btrieve* file on the Novell® BorderManager™ server and is maintained by CSAUDIT.NLM. The access log cannot be edited or manipulated from the server; however, the data can be exported for analysis. The format of the exported data is compatible with trend analysis software packages, such as WebTrends*.

There are two ways to export the access control log from NetWare® Administrator:

- “Exporting Data from the Access Control Users Statistics Window” on page 6
- “Exporting Data Using the Export Logs Option” on page 8

If you use the second method, you can also combine the audit log files from other BorderManager services with the access control log into a single ASCII file.

Exporting Data from the Access Control Users Statistics Window

To export records from the Access Control Users Statistics window, complete the following steps:

1. **In NetWare Administrator, click the server object representing the BorderManager server.**
2. **Select Novell BorderManager from the Tools menu.**
3. **From the BorderManager menu, select View Access Control Log.**
4. **Click Display Records, enter the dates for the records you want to display, and click OK.**
5. **In the Access Control Users Statistics window, click Export Data and enter the path and filename, or click Browse to select the destination of the export file.**

6. **Select one of the following sort formats under Information Output Selection and click OK:**

    - Entry Time (connection by connection)—(Default selection) Sorts records from the earliest entry time to latest entry time.
    - Access by users—Sorts records in alphabetic order based on the user's NDS™ username.
    - Access by hosts—Sorts records in ascending order (for IP addresses) or alphabetic order (for DNS hostnames).

7. **(Conditional) If the export filename already exists under the directory path selected, you are prompted to replace the file. Click Yes to overwrite the file or No to specify the destination as described in Step 5.**

The record fields are written to disk with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported data has the following format:

- Entry Time—Time connection was established.
- Username—NDS name or IP address of the user.
- Access—Action specified in the access rule for this connection: either Allowed or Denied.
- Protocol—Protocol string representing the port number used for the connection: HTTP, FTP, HTTPS, and so on. For example, HTTP represents a connection made using port 80.
- Hostname—DNS name or IP address of the accessed host.
- Service—Service used to access the host: Proxy Services or Novell IP Gateway.
- Rule Number—ID number of the rule that grants or denies access to the hosts.

Exporting Data Using the Export Logs Option

The procedure to export access control data using the Export Logs option from the BorderManager pull-down menu extracts the same data from the Btrieve database, but offers additional export options that cannot be activated from the Access Control Users Statistics window.

To export the access control log, complete the following steps:

1. **In NetWare Administrator, click the server object representing the BorderManager server.**

2. **Select Novell BorderManager from the Tools menu.**

3. **From the BorderManager menu, select Export Logs.**

4. **Click Set Range to enter the date range.**

   This is the range of dates comparable to the dates used to display records in the Access Control Users Statistics window. The default range is the current server date.

5. **Click Browse to select the drive mapped to the destination for the export file.**

   This is the path and filename for the export file. The default destination is A:\YYYYMMDD.LOG, where YYYY is the current year, MM is the current month, and DD is the current day. If you change the filename from the default format, the filename will not reflect the current server date. For example, if you change the filename format to MMDDYYYY.LOG, the next time you try to export logs on another day, the log filename will not have incremented to the current date.

6. **(Optional) If the default filename is unacceptable, enter the filename in the File field.**

7. **(Optional) If you want to combine the access control log with audit logs from other BorderManager services, check the Combine Log Files check box.**

   This feature allows log files from different services to be combined into a single output file. When log files are combined, they are appended to one file, service by service.

8. **Under Log Selection, check the box for ACL.**

   If the Combine Log Files feature has been selected, check all the services whose data will be combined into the export log file.

9. **(Optional) If you checked Combine Log Files in Step 7, under Log Selection, check all other BorderManager services audit log files to be combined with the access control log file.**

10. **Click OK.**

The access control log is exported to an ASCII file. The record fields are written with a tab as the delimiter. Each record ends with a carriage return and line feed. The exported access control data has the following fields:

- Keyword—ACL. If the Combine Log Files option was selected, the keyword is at the beginning of each line from the access control list (ACL) audit log.
- Date.
- Time.
- Source—Typeless NDS name and context, such as mlira.pubs.novell, or an IP address.
- Destination—Domain name or IP address.
- Bytes received.
- Status—Allow or Deny.
- Protocol—Protocol used, such as HTTP or FTP.
- Service—Service used to access the host: Proxy Services or Novell IP Gateway.
- Rule ID—An 8-digit hexadecimal number that identifies the rule associated with the allowed or denied access.

If the Combine Log Files feature is *not* selected and you select one or more services under the Log Selection field, a separate export file is created for each service under a subdirectory of the export destination path.

The export subdirectories used are shown in the following table.

Log Type	Export Subdirectory
HTTP Proxy	HTTP
FTP Proxy	FTP
NNTP Proxy	NNTP
Mail Proxy	SMTP
RealAudio* and Real Time Streaming Protocol (RTSP) Proxies	RAUDIO
DNS Proxy	DNS
Generic Proxy	GENERIC
SOCKS Client	SOCKS
IPX Gateway (Novell IP Gateway)	IPXGW
VPN	VPN
ACL (access control)	ACL

For example, if you specified an export destination of VOL1:LOGS\19981019.LOG, did not select the Combine Log Files feature, and checked the boxes for HTTP Proxy, SOCKS client, and ACL, the following log files would result:

- VOL1:LOGS\HTTP\19981019.LOG
- VOL1:LOGS\SOCKS\19981019.LOG
- VOL1:LOGS\ACL\19981019.LOG