VERSION 3.5

Alerts

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.

Alert
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

USRobotics is a registered trademark of U.S. Robotics, Inc.
WebTrends is a trademark of WebTrends Corporation.
Windows is a registered trademark of Microsoft Corporation.
Windows 95 is a trademark of Microsoft Corporation.
Windows 98 is a trademark of Microsoft Corporation.
Windows NT is a registered trademark of Microsoft Corporation.
X Window System is a trademark of Massachusetts Institute of Technology.

The RSA logo is a trademark of RSA Data Security, Inc.

GENUINE
RSA™
ENCRYPTION ENGINE

Contents

About This Guide

1 Managing Alert Messages

About This Guide

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

This documentation provides the following additional information: “Managing Alert Messages” on page 1—Descibes how to view alert messages and how to respond to them.

x Alert

chapter

1 Managing Alert Messages

This chapter describes how to view alert messages generated by Novell® BorderManager™ Alert and how to respond to them. It contains the following sections:

- "Viewing Alerts Sent as E-mail Messages" on page 1
- "Viewing Alerts in the Audit Trail Log File" on page 2
- "Viewing Alerts in the Console Log" on page 4
- "Responding to Alerts" on page 4

Viewing Alerts Sent as E-mail Messages

All e-mail notifications triggered by BorderManager™ Alert contain a time stamp, the name of the server where the event occurred, the service affected, and an error message.

Note When the message is sent to a pager, the time stamp, server name, and error message appear first, followed by the sender, recipient, and subject. This is done to accommodate paging services that limit the amount of alphanumeric text that is displayed.

In the sample e-mail message that follows, substitute your own Domain Name System (DNS) domain name for novell.com:

From: <nbmalert@novell.com>

To: <admin_1@novell.com admin_2@novell.com>

Subject: The system is short on disk space and operations may fail

Time: 7-17-98 9:45:07am

Server: SJ-NW5

Service: NetWare Operating System

The system is short on disk space and operations may fail

Note If a loaded NetWare Loadable Module™ (NLM™) causes the alert, the e-mail message might not always identify the offending NLM because the NLM that detected the error might be reported instead. Therefore, load MONITOR.NLM to check any unusual statistics if the cause of the alert is not clearly evident.

If BorderManager Alert has been configured and e-mail notification fails to occur when alerts are displayed on the server console, verify the following:

- The alert condition has been enabled for notification in NetWare® Administrator.
- All e-mail addresses configured for the BorderManager server are for valid accounts.
- The primary and backup e-mail servers have e-mail forwarding enabled.
- The primary e-mail server or at least one backup e-mail server is up and running.
- All NDS™ partitions have been synchronized if the alert configuration was recently changed. A delay in synchronization can mean that your server has not been updated with the latest configuration, especially if the alert configuration applies to an entire organization.
- A route to the mail server has been established. Ping the mail server from the BorderManager server and inspect the trace on the route.
- There are no filters on routers between the BorderManager server and the mail server that deny Simple Mail Transfer Protocol (SMTP) traffic.

Viewing Alerts in the Audit Trail Log File

BorderManager™ Alert logs server events in the audit trail log file. The alert record contains information such as the type of alert, a description of the event, the name of the server that generated the alert, and a time stamp. Use the audit trail log file to check for anomalies or suspicious activities that affect routing and security on your network.

The audit trail log file, CSAUDIT.LOG, is maintained by CSAUDIT.NLM. The audit trail log file is managed with the CSLIB audit trail utility. Use this utility to view records in the audit trail log and configure a schedule for archiving the log. The active audit trail log file is located in SYS:SYSTEM\CSLIB. Archived audit log files are located in SYS:SYSTEM\CSLIB\LOGS.

This section contains the following procedures:

- "Displaying Audit Trail Log Records with the Audit Trail Utility" on page 3
- "Archiving the Audit Trail Log File" on page 3

Displaying Audit Trail Log Records with the Audit Trail Utility

To view the audit trail log file, complete the following steps:

1. **To run the CSLIB audit trail utility from the server console, enter**

   CSAUDIT

2. **Select Display Audit Trail Records.**

   The currently active log file is displayed. If the current log file has the record you need, you are done. Otherwise, to view an archived log file, continue with Step 3.

3. **Press** Insert **to view the other display options.**

4. **From the Display Options menu, choose Select from Archived File List.**

5. **Use the** Up-arrow **and** Down-arrow **to locate the archived log file to view.**

6. **Press** Enter **to view the records in the log file.**

7. **Press** Esc **until you are prompted to exit the audit trail utility.**

Archiving the Audit Trail Log File

As with most log files, the audit trail log file can grow rapidly. Because the audit trail log file is stored on the SYS: volume, it is important to archive it and rotate the archived log files on a regular basis.

To configure the frequency of archiving and the number of archived log files, complete the following steps:

1. **From the server console, enter**

   CSAUDIT

2. **Select Audit Trail Configuration.**

3. **Press** Enter **in the Archive Hour field and select the hour at which the audit trail log file should be archived.**

4. **In the Archive Interval field, enter the number of days for which the active audit log file records data.**

5. **In the Archive Files Retained field, enter the number of audit log files that will be archived before the first archived file is overwritten.**

6. **Press** Esc **and select Yes to save the changes.**

7. **Press** Esc **until you are prompted to exit the audit trail utility.**

Viewing Alerts in the Console Log

Because BorderManager™ Alert sends alert messages to the server console, if CONLOG is running on the server, the alert message is also saved in SYS:ETC\CONSOLE.LOG.

To view the console log at the server console, enter

LOAD EDIT SYS:ETC\CONSOLE.LOG

Responding to Alerts

BorderManager™ Alert monitors server performance, license acquisition for licensed BorderManager services, security, and Proxy Services availability.

For information on specific alerts, refer to the following:

- "Server Performance Alerts" on page 6

- "License Acquisition Alerts" on page 7

- “Security Alerts” on page 7
- “Proxy Alerts” on page 10

The following table describes some recommended responses to the BorderManager alerts.

Alert	Recommended Actions
Disk space shortage	Reduce the size and number of log files. Add more disk space, if necessary.
Memory shortage	Check server resources using MONITOR.NLM to determine whether a module is using excessive memory. Add more memory, if necessary. Depending on the bus type, some NetWare® servers do not register all the memory present unless a REGISTER MEMORY statement exists in the STARTUP.NCF file. More information about REGISTER MEMORY is located in the NetWare 5™ online documentation at the following path: Reference > Utilities Reference (under the General Reference heading) > Utilities > REGISTER MEMORY
ECB shortage	Check server resources using MONITOR.NLM to determine which NLM uses the most event control blocks (ECBs). Increase the maximum packet receive buffers on the server if server memory allows.
License error	Verify the current licenses installed for the server and check for license conflicts or expired trial licenses. Install additional licenses, if necessary.
Loading or unloading a security-sensitive NLM	This alert is primarily informational. Verify that the server console is secure and all remote sessions are authorized. Reload or unload the NLM, if necessary.
Oversized ping packet	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block pings originating from that source.
SYN packet flooding	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block TCP packets originating from that source.

Alert	Recommended Actions
Oversized UDP packet	Use a packet sniffer to capture packets and determine the source IP address. Configure a TCP/IP packet forwarding filter to block UDP packets originating from that source.
Cache hierarchy parent (ICP parent) down	Ping the parent server to check if there is a routing problem. Verify that the parent server for the cache hierarchy is down and bring the server back up. Note that if the cache hierarchy has multiple parents configured, proxy servers lower in the hierarchy will use the other parent servers while this server is down.
SOCKS server down	Ping the SOCKS server to check if there is a routing problem. Verify that the SOCKS server is down and bring the server back up.
POP3 or SMTP server down	Ping the Post Office Protocol 3 (POP3) or SMTP server to check if there is a routing problem. Verify that the POP3 server or internal mail server is down. You might not be able to resolve this problem if the POP3 server is administered by someone who is outside your organization.

Server Performance Alerts

Server performance alerts notify you of potential problems with server parameters or operations that can cause BorderManager services to underperform or fail.

The server performance alerts are as follows:

- Disk space shortage

  A disk space shortage warning indicates that the shortage of disk space is severe enough to potentially cause server operations to fail.

- Memory shortage

  A memory shortage warning indicates that the shortage of memory is severe enough to potentially cause server operations to fail.

- Event control block (ECB) shortage (out of receive buffers or no ECBs available)

An ECB shortage warning indicates that the packet receive buffer or ECB shortage is severe enough to potentially cause network input or output to degrade or fail.

License Acquisition Alerts

A license alert indicates that a BorderManager service was unable to acquire the license it needs to operate.

BorderManager Alert monitors license acquisition for the following:

- Proxy Services
- Novell IP Gateway
- Virtual Private Network (VPN) servers and clients
- Access control

Security Alerts

Security alerts notify you of possible security breaches. The causes of these alerts should be investigated further because your server might be the target of a denial-of-service attack.

Denial-of-service attacks commonly plague servers connected to the Internet and are initiated by someone without authorized access to servers. A denial-of-service condition can be caused by a bombardment of packets sent to a server that consumes significant memory or CPU processing time. After these server resources have been allocated to handle the packets, connection requests made by legitimate users cannot be processed effectively.

As with computer viruses, new denial-of-service attacks are launched on the Internet community without warning. Many of the known denial-of-service attacks are documented on various Web sites.

The BorderManager security alerts include the following:

- Loading or unloading a security-sensitive NLM

  Security-sensitive modules are those that can potentially compromise network or server security when they are loaded or unloaded.

The modules that are considered security-sensitive are

  - DS.NLM
  - FTPSERV.NLM
  - IPXIPGW.NLM
  - PROXY.NLM
  - REMOTE.NLM
  - TFTPSERV.NLM
  - VPNINF.NLM
  - VPMASTER.NLM
  - VPSLAVE.NLM

- Oversized ping packet

  An oversized ping packet warning can indicate that malicious activity is occurring on the server. Pings with an abnormally large packet size are a symptom of a denial-of-service attack known as the Ping of Death. This alert is generated when the server receives and discards ping packets that have more than 10,240 bytes of data. The server is enabled to discard these packets by default.

  For certain situations which require your server to receive larger ping packets, such as router stress tests, enter the following SET commands at the server console to change the largest ping packet size or disable packet discarding:

  SET LARGEST PING PACKET SIZE=*n*

  SET DISCARD OVERSIZED PING PACKETS=OFF

  The variable *n* is a decimal number representing the number of bytes allowed. Never specify a number with commas.

  To reenable packet discarding, enter the following command at the server console:

  SET DISCARD OVERSIZED PING PACKETS=ON

Note Because packet sizes are limited by the type of media used, you should know your network topology before changing the largest ping packet size. For Ethernet only, the oversized ping packet alert is not generated if the largest ping packet size is set between 35,541 and 65,535 bytes. However, alerts are generated for packets smaller than 35,541 bytes. The acceptable packet size ranges for other media differ and depend on each medium’s maximum transmission unit (MTU)—the largest packet size a medium can transport without fragmentation.

- SYN packet flooding

  A TCP SYN packet flood warning can indicate that malicious activity is occurring on the server which can cause a denial-of-service condition. TCP connections require a three-way handshake between the server and client: 1) the client sends a packet in which the SYN flag is set in the TCP header, 2) the server sends a SYN/ACK (acknowledgment) packet, and 3) the client sends an ACK packet so data transmission can begin. A denial-of-service condition occurs when the client fails to send the last ACK packet and intentionally sends successive TCP connection requests to the server to fill up the server's buffer. After the server's buffer is full, other clients cannot establish a connection, resulting in a denial-of-service condition.

Important BorderManager Alert detects only SYN packet floods for socket applications, such as FTP.

  Due to the importance of defending your server against SYN packet floods, the detection of SYN packet floods should always be enabled. However, for extreme troubleshooting measures, use the following SET command to disable detection if necessary:

  SET TCP DEFEND SYN ATTACKS=OFF

  Reenable detection with the following command:

  SET TCP DEFEND SYN ATTACKS=ON

- Oversized UDP packet

  An oversized UDP packet warning can indicate that malicious activity is occurring on the server. This alert is generated when the server receives and discards UDP packets larger than 16,384 bytes. The server is enabled to discard these packets by default.

  If necessary, enter the following SET commands at the server console to change the largest UDP packet size or disable packet discarding:

  SET LARGEST UDP PACKET SIZE=*n*

  SET DISCARD OVERSIZED UDP PACKETS=OFF

The variable *n* is a decimal number representing the number of bytes allowed. Never specify a number with commas.

To reenable packet discarding, enter the following command at the server console:

SET DISCARD OVERSIZED UDP PACKETS=ON

Note Because packet sizes are limited by the type of media used, you should know your network topology before changing the largest UDP packet size. For Ethernet only, the oversized UDP packet alert is not generated if the largest UDP packet size is set between 35,541 and 65,535 bytes. However, alerts are generated for packets smaller than 35,541 bytes. The acceptable packet size ranges for other media differ and depend on each medium's MTU—the largest packet size a medium can transport without fragmentation.

Many other documented denial-of-service attacks can be detected by BorderManager Alert, although attacks are not identified by name. For example, although the preceding list of alerts does not include a specific alert for the Smurf, Teardrop, or LANd attacks, they are easily detected. The Smurf attack uses an Internet Control Message Protocol (ICMP) echo in response to ping broadcasts to flood a server. The Teardrop attack intentionally overlaps fragments to cause errors in fragment reassembly, resulting in the packets being resent repeatedly. The LANd attack sends packets with the same source and destination address, resulting in an endless loop of packets being sent to the server.

Proxy Alerts

Proxy alerts generally indicate that a proxy server has not been configured correctly or is down.

The proxy alerts are as follows:

- Cache hierarchy parent (ICP parent) down

  A cache hierarchy parent down warning indicates a problem with the parent proxy cache server in a configured cache hierarchy. If the cache hierarchy client is enabled on the proxy server and the proxy fails to connect to the parent, the alert will be triggered. If the option to forward all requests through the hierarchy has been selected and the parent is down, requests that cannot be fulfilled through the cache can result in an error because the parent is not available to access the source information.

- SOCKS server down

A SOCKS server down warning indicates that the SOCKS server to which the proxy cache server connects as a client is down. If the SOCKS client is enabled on the proxy server and the proxy fails to make a connection, the alert will be triggered. Because a SOCKS server is often used as a firewall, requests that cannot be fulfilled through the cache can result in an error because the proxy cannot forward requests through the firewall.

- POP3 or SMTP server down

  A POP3 server down warning indicates that there is a problem with a POP3 server or an internal SMTP mail server. The mail proxy enabled on the BorderManager server cannot forward outgoing mail to the POP3 server or deliver incoming mail to the SMTP server.