



INTELLIGENT EVENT MODULE BASICS

The VERITAS NetBackup 5.0 Intelligent Event Module (IEM) enables you to automate real-time monitoring of the VERITAS NetBackup application from Symantec™ and capture the critical information you need for effective enterprise backup and recovery management.

The VERITAS NetBackup 5.0 IEM provides ConsoleWorks® with a watch-list of text messages, including error codes, system warnings, and status alerts, produced by NetBackup 5.0. ConsoleWorks watches for these messages, called Events, in the data streams of your managed applications.

Events

When ConsoleWorks detects an Event, it alerts you to the Event as it is happening, records the circumstances surrounding the Event, and automatically performs the default or customer-configured responses associated with that Event.

Scans

IEMs come with Events pre-arranged in logical groupings, called Scans™. Working with a Scan—or a combination of Scans—instead of hundreds of individual Events simplifies managing Events across your enterprise.

VERITAS NETBACKUP 5.0 IEM AT A GLANCE

Events:	746
Scans:	1 Master 5 Event Severity
Filename:	<code>cw_iem-symantec_netbackup-0002.bin</code>
License Required:	<code>CONWRKS-DB-NETBACKUP.lic</code>
Connector Required:	Syslog

USING THE VERITAS NETBACKUP 5.0 IEM

To use this IEM, complete the following tasks:

1. Download the IEM from the TDi web site.
2. Import the IEM into ConsoleWorks.
3. Associate the Scans from the IEM with the applications you want to manage.

To Download the IEM

1. Install the license for the VERITAS NetBackup 5.0 IEM. To obtain this license, contact your TDi Solutions Team Manager (sales@tditx.com).
2. Move to the TDi web site (www.tditx.com/support_iemdownloads.asp).
3. On the Product Downloads page, locate and click **Symantec (VERITAS) NetBackup 5.0**.
4. In the Connect to support2.tditx.com dialog box, enter your User name and Password, and click **OK**. To obtain a User name and Password, contact TDi Support (support@tditx.com).
5. Save the file (`cw_iem-symantec_netbackup-0002.bin`) to a directory accessible from your client workstation.

To Import the IEM

1. On the ConsoleWorks main menu, click **Admin > Database > Import IEM**.
2. On the Import IEM page, click **Browse**.
3. On the Choose file dialog box, locate and double-click `cw_iem-symantec_netbackup-0002.bin`.
4. On the Import IEM page, click **Import IEM**, and wait for the **IEM import completed** message to appear on the page before associating the IEM's Scans.

To Associate the Scans

Associate the Scans with the VERITAS applications you want ConsoleWorks to monitor. When you associate Scans with an application, you are specifying that ConsoleWorks scan the data streams of that application for the Events contained in the Scans.

Example: To associate the NETBU_CRITICAL Scan

1. On the ConsoleWorks main menu, click **Manage > Scans > Show Scans**.
2. On the Show Scans page, in the Scans column, click **NETBU_CRITICAL**.
3. On the Scan: NETBU_CRITICAL page, in the Unassociated Consoles column, select the check boxes next to the names of the managed applications you want to associate with the Scan.
4. Click **Update Scan**.

For detailed instructions on associating Scans, please refer to the ConsoleWorks user's guide.



SCANS AVAILABLE IN THE VERITAS NETBACKUP 5.0 IEM

The VERITAS NetBackup 5.0 IEM contains a Master Scan and five Event Severity Scans.

Master Scan

The Master Scan, **NETBU**, is the top-level Scan. It references all the other Scans in the IEM. When you associate the Master Scan with an application, you are specifying that ConsoleWorks scan the data streams of that application for any of the IEM's 746 Events.

Event Severity Scans

The VERITAS NetBackup 5.0 IEM contains five Event Severity Scans. Use one or more of these Scans to monitor VERITAS applications for Events based on their Severity level.

The IEM provides the following Event Severity Scans:

• NETBU_CRITICAL	28 Events
• NETBU_MAJOR	8 Events
• NETBU_MINOR	79 Events
• NETBU_WARNING	595 Events
• NETBU_INFORMATIONAL	36 Events

SAMPLE VERITAS NETBACKUP 5.0 IEM EVENTS

The VERITAS NetBackup 5.0 IEM provides you with names, message texts, Severity ratings, status codes, explanations, and recommended responses for Events produced by NetBackup 5.0.

This section displays samples of the information you receive for each Event in the VERITAS NetBackup 5.0 IEM.

Sample Event 1

Name: NETBU_VOLUMEUSE

Message: Volume is in use

Severity: INFORMATIONAL

Robotic

Status Code: 237

Explanation: The media was in use.

Response: Use the robot test utility or a vendor administrative interface to verify the status of media. Determine what applications may be using the media. Dismount the media if it is not being used by an application. Wait for the media to become available, as needed.

Sample Event 2

Name: NETBU_NONEREQUESTEDFILES

Message: none of the requested files were backed up

Severity: CRITICAL

Status Code: 2

Explanation: A backup or archive could not back up any of the files in the file list.

Response: Verify that the files exist and you have read access to them. Also, perform the following checks:

- Check to see if there is a trailing space on one or more of the filenames in the client's file list. Remove any inadvertent trailing characters (such as spaces or tabs).
- On UNIX clients, check to see if the files or directories would be excluded because of an entry in `/usr/openv/netbackup/exclude_list`.
- On PC clients, check the exclude list per the instructions in the user's guide for the client.
- On Windows clients, verify that the account used to start the NetBackup Client service has read access to the files.
- If you are backing up a network drive or a UNC (universal naming convention) path, use the Services application in the Windows Control Panel to verify that the NetBackup Client service does not start under the SYSTEM account. The SYSTEM account cannot access network drives.
- To back up network drives or UNC paths, change the NetBackup Client service startup to log in as a user that has permission to access network drives.

© 2007 TECSys Development, Inc. The information in this document is provided by TECSys Development, Inc. as-is without warranty of any kind and is subject to change without notice. The warranties for TECSys Development, Inc. solutions are set forth in the limited warranty statements accompanying such solutions. Nothing herein shall be construed as constituting an additional warranty. All products or company names mentioned in this document are trademarks or registered trademarks of their respective owners. Portions of the technology within the ConsoleWorks server are protected under US Patent number 6,505,245. ConsoleWorks is a registered trademark of TECSys Development, Inc.