IBM Tivoli Risk Manager Version 4.1 Fix Pack 3

Date: December 5, 2003

Name: 4.1-RMG-FP03

Component: IBM Tivoli Risk Manager Version 4.1

Before using this information and the product it supports, read the information in the "Notices" section, at the end of this document.
First Edition (December 2003)
This edition applies to version 4, release 1 of IBM Tivoli Risk Manager.

Table of Contents

1. Installation Notes

This IBM Tivoli Risk Manager fix pack supercedes all previous patches and fix packs for the AIX, Solaris, Linux and Windows operating systems.

In order to install this fix pack on the HP-UX operating system, 4.1-RMG-FP02 must be installed first.

The Tivoli Risk Manager fix pack is provided as an InstallShield Multiplatform installation on the AIX, Solaris, Linux, HPUX, and Windows operating systems. The included files are:

riskmgr_patch03.jar	(Java jar file that contains the fix pack files)
riskmgr_patch03_aix	(launcher executable for installing on AIX)
riskmgr_patch03_hpux	(launcher executable for installing on HPUX)
riskmgr_patch03_linux	(launcher executable for installing on Linux)
riskmgr_patch03_solaris	(launcher executable for installing on Solaris)
riskmgr_patch03_win.exe	(launcher executable for installing on Windows)

Before installing the Tivoli Risk Manager fix pack on an HP-UX system, stop Web IDS and any other processes that use Tivoli Risk Manager Perl. If Tivoli Risk Manager Perl support is running when you install the fix pack on an HP-UX system, the installation will not be successful.

This fix pack can be installed using one of the following methods:

1. Run the launcher executable by entering the following command:

   riskmgr_patch1_<platform name>

2. Use the Java jar file and run the following command:

   java -cp riskmgr_patch1.jar run

Refer to the IBM Tivoli Risk Manager User's Guide for additional installation options.

To install the Tivoli Risk Manager fix pack on the Linux for zSeries platform, use the RPM packages provided, which contain the fix pack updates. These packages should be installed by running the following command:

rpm -F <package_name>

1.1 Additional Installation Instructions

The following files, located in the etc/templates directory, have been updated in this fix pack and should be copied into the etc directory to enable the update. If you have customized any of these files in your environment, you should keep a backup copy of the file before copying the updated file into the etc directory and then merge in your customizations.

etc/templates/baroc/sensor_abstract.baroc
etc/templates/webids.cfg
etc/templates/webids.fmt
etc/templates/webids.nt.fmt

After updating the sensor_abstract.baroc file, you will need to run the rmcorr_cfg -update command on your event server systems. Then you must restart the agent on your distributed correlation server systems to enable the change.

After updating the webids.fmt or webids.nt.fmt files, regenerate the .cds file using the wrmcrtcds command.

2. APAR and Defect Solutions Included With This Fix Pack

The following sections contain explanations and solutions for the problems fixed in this fix pack. Internal defect numbers and external APAR numbers (when available) are provided for your reference.

Defect 30310 - NIDS sending malformed events causing the correlation engine to hang
PROBLEM DESCRIPTION:
NIDS Sending malformed events causing the correlation engine to hand. This is a result of NIDS not properly setting the source and destination address fields. This only occurred for undefined events, ie: events that did not match any leaf node or other format.
SOLUTION:
Modify the undefined event format to default source and destination address fields to the sensor address.

Defect 30439 - Correlation engine hangs if a malformed event comes in from the agent
PROBLEM DESCRIPTION:
(Customer View) The engine queue will appear to hang. Events will not flow through the Risk Manager Agent.
(Actual) The engine queue failed to respond properly to events that are missing either a source or destination setting. With this fix, events that do not contain the required attributes will not cause the engine's queue to appear to hang.
SOLUTION:
Modified the file rmagent.jar so that the missing attributes will not cause the queue to hang.

APAR IY40923 - PIX Events not parsed by TEC and not archived by DB_Sender
PROBLEM DESCRIPTION:
(Customer View) PIX Events not being parsed by TEC and not archived by DB_Sender
(Actual) Adaptor is sending malformed events to DB_Sender
SOLUTION:
The ideal solution to this problem is to fix the adapter that sends malformed events to the RM_Agent. Since this type of problem may be experienced by multiple customers and the agent event normalization code can be updated to detect when an expected attribute of an RM_SensorEvent is incorrectly formatted to have brackets around the value, the code will be added to perform this check.
With this fix, the normalization code will:

A. Log the malformed event to the log of the local machine.
B Generate an RMAgent_InvalidEvent event (which is an RM_SensorEvent)

Changes made to the rmagent.jar file.

Defect 31626 - Wrmadmin hangs with XP firewall adapter
PROBLEM DESCRIPTION:
(Customer View) I installed RM 4.1 client (Patch 1) on a Windows XP Professional system. I am running Windows event log adapter and XP firewall adapter, which is a Perl script that calls RM EIF via the Perl module (rmadpm). Both the logfile and XP firewall adapter are using summarization rules in the local agent.
The XP firewall (downloaded from our Web support site) reads from the XP firewall log (a text file), generates unformatted log entries and then calls rmadpm_send_message($logstring, 0). At the same time, I modified the adapter so it would output each log entry to STDOUT as it calls rmadpm. The adapter reads until the end of the firewall log, then sleeps for a second, then attempts to read from EOF, ad infinitum.
What I've observed is that when the XP firewall adapter completes its initial pass through of the firewall log and has sent off a number of events via RM EIF, the system goes into a "steady state" where no more new events are being generated. After waiting for "some time" (more than a few minutes, up to half an hour), when I execute 'wrmadmin -info' from a command line, the cursor moves to the next line but no output is generated and no command prompt is presented, as if wrmadmin is hanging. If I Ctrl-C to get out of the program, the command prompt returns and I can re-issue the 'wrmadmin -info' command, to which the program responds immediately with the expected output ("Agent is active.") ALSO, after the afore-mentioned Ctrl-C, the XP firewall adapter suddenly becomes active and starts sending a burst of events until EOF of the firewall log file.
After that, if you again do nothing and wait for 'some time', the above scenario can be reliably repeated when you try to execute 'wrmadmin -info'.
(Actual) Windows code incorrectly resetting semaphore state, resulting in an intermittent block on a syncronization semaphore.
SOLUTION:
Incorrect usage of semaphore call resulted in setting a sycronization semaphore to a blocked state on wrmadmin exit. Next usage of wrmadmin would hang. Changed common shared library code to correctly set semaphore state to exit.

APAR Y41545 - Risk Manager having problems with Single Port BDT due to defect with TEC 3.8
PROBLEM DESCRIPTION:
Problems with Single Port BDT. Caused by a bug in the TEC java eif code Risk Manager uses. RMAgent fails when used Single Port BDT.
SOLUTION:
An updated evd.jar that contains the fix was provided by TEC support.

Defect 32010 - Changed character set values for Sybase on HP w/ TEC and RM
PROBLEM DESCRIPTION:
Information on character set values with Sybase on the HP-UX system.
SOLUTION:
(Readme Help Inclusion)
If you are planning to use a Sybase database on an HP-UX system with the Tivoli Enterprise Console and the Tivoli Risk Manager Archive Table, certain Sybase parameters will need to be changed during installation. During the installation of the Sybase server be sure to select UTF8 as the default character set instead of HP Roman 8.
After installing the Tivoli Enterprise Console and using the Tivoli Enterprise Console Database Assistant to create the Tivoli Enterprise Console database, do the following to disable the character set conversion:

1. Enter the isql utility using the sa account and password.

   isql -U sa -P sa password -S server

2. Run the following commands:

   sp_configure "disable character set conversion", 1
   go

3. Exit from the isql utility by using the exit command.
4. Stop and restart the Sybase server.

Defect 33916 - Summarization will not replace message attribute
PROBLEM DESCRIPTION:
Summarization will not replace msg attribute unless it is specifically set in format file. Some summarized events are missing some of the SET:attribute=value specified in the summarization rules. Particularly, any attribute that was not set by the sensor/adapter in the event, was not set by the summarization action.
SOLUTION:
Some summarized events are missing some of the SET:attribute=value settings

specified in the summary rule. The summary action only set attributes that the sensor/adpater had included in the events being summarized. With this fix, all attributes specified in the summary rule will be set on the resulting summary event.

Defect 33980 - Set date_reception to the current time
PROBLEM DESCRIPTION:
This problem only occurs in manually configured systems in which a RMAgent is writing to the archive table, but not performing correlation/normalization. With this atypical set-up, events may not be written to the archive table because the date reception attribute is not included in the event information passed between Risk Manager agents.
SOLUTION:
The event's date_reception field in the archive table will be set to the current time of the system where the agent performing the database write is running. This occurs if and only if the date reception is not set as part of the event information.

Defect 34032 - Relink webids.nt.fmt to webids.fmt between RM 4.1 and RM 4.2
PROBLEM DESCRIPTION:
Relink webids.nt.fmt to webids.fmt between RM 4.1 and RM 4.2
SOLUTION:
Backport complete.

Defect 34062 - Double <predicate>true</predicate> definition
PROBLEM DESCRIPTION:
The file monitor_heartbeat_rules.xml has double definitions for the following predicate:

<predicate>true</predicate>

Presumably one would suffice.
SOLUTION:
Added a passthrough rule with the same timeInterval, etc to reset the heartbeat rule and itself. This alleviates the problem of not identifying missing heartbeat events.

Defect 34232 - Event toString method needs to quote values with embedded
PROBLEM DESCRIPTION:
Event toString method needs to quote values with embedded '='. Events with attributes that contain embedded equal sign characters appear to be lost. It is arguable that the events are malformed and should be thrown out, but since there are some Risk Manager adapters that create events with embedded equal signs in the attribute values and having the agent enclose such values in single quotes will allow the events to be processed, changing the agent to quote such values is a reasonable way to alleviate the problem.
Note: This will not fix the problem of such events being lost when not routed through a Risk Manager Agent.
SOLUTION:
This defect fixes a problem where some events are discarded as invalid because their attribute data includes embedded equal sign (=) characters which cause the events to fail to be parsed. Additional fix (defect 34479) of not quoting numeric values added to the rm410 track of this defect.

APAR IY44978 - RM_Agent hangs when an event is split into 2 different IP Packets
PROBLEM DESCRIPTION:
Problem caused by bug in the TEC java EIF code used by the RM_Agent to send and receive events data. In the event that an event was split into two or more IP packets, RM_Agent would stop running.
SOLUTION:
This problem was fixed by inclusion of the latest evd.jar via TEC support.

Defect 35302 - Added support for the PIX Firewall version 6.3

Defect 36289 - Circumvent db2 batch size restrictions
PROBLEM DESCRIPTION:
Archive db sender with batching enabled fails miserably on db2 since statement size is restricted to 64k bytes.
SOLUTION:
As above. When the insert SQL for a set of events is larger than 64K bytes, the insert fails. Batching code changed to ensure that the size of the insert statement is < 64K.

APAR IY45953 - RM_Agent hangs when experiencing "Out of Memory" condition

PROBLEM DESCRIPTION:
The Risk Manager Agent sometimes is not able to keep up with the event traffic, which results in many events queueing at the agent. When this happened, the agent's memory usage grew until no more memory was available for its use. At that point, an out of memory exception is thrown by the Java Virtual Machine. This caused the agent to appear to hang. Any attempt to restart the agent without first clearing events from the persistence directory caused the problem to recur.
SOLUTION:
The agent's queueing mechanisms was changed to alleviate the memory over-consumption problem. Additionally, the agent's persistence mechanism was changed to be more efficient, which should alleviate the symptom of many events queueing. Additionally, some fixes to the EIF transport used by the agent to route events were also included in this defect.
Notes:
1. The contents of the persistence directories is significantly changed with this fix. Any residual .RMG files will not be processed by the agent.

2. It is still possible during an event flood for the agent to not be able to keep up with the flood of events. Over time, the agent will process these events.

3. It is still possible, although much less likely, for the agent to experience an out-of-memory exception. If you expect a large event volume to pass through your agent, please configure the agent's available memory to a sufficiently large number. To change the available memory, edit $RMADHOME/etc/rmad.conf add (or change) a line similar to the following:

RmagentMemMax=92160000

Defect 36926 - SQL0803 in HRM_c-5_s030_Load_Comp
PROBLEM DESCRIPTION:
SQL0803 error occurs in ETL1 step HRM_c05_s030_Load_Comp when attempting to insert HRM_CLASSCAT attributes in the TWG.CompAttr. The records being inserted violate an index constraint on the table which requires a unique value for columns COMP_ID+ATTRTYP_CD+COMPATTR_STRT_DTTM.
Further investigation shows that the HRM.Transform_Events table, created by the previous ETL1 step, had 2 records with the same destination host, class category and source host, but the source host was in the src_hostname column in one record and in the src_ipaddr column in the other record. When these values were extracted from HRM.Transform_Events into session.temp_rm_classcats, they produced duplicate records. When the duplicate records were inserted into TWG.CompAttr, the SQL0803 error resulted.
SOLUTION:
Code fix to account for this to be included in FP 0003.

Defect 37204 - Removed librmad.so exit functions for IGS adapter support
PROBLEM DESCRIPTION:
The object file librmad.so contains exit and _exit functions in the TEC code. This is causing problems with the IGS adapter.
SOLUTION:
Removed libmad.so exiting functions. Include with FP 0003.

Defect 37815 - Wrmadmin -k killed webids process (TEC Defect 163189)
PROBLEM DESCRIPTION:
While webids is running, start wrmadmin -r and type wrmadmin -i. After about 2 -5 minutes, webids gets killed and the info form wrmadmin -i came out incorrect.
SOLUTION:
This problem has been traced to the TEC EIF "C" api code used to send event data. If an application using this api is processing large volumes of event data and is disconntcted, the application will seg. fault in tec_put_event when the EIF api attempts to reconnect.
This problem is related to the RetryInterval used by the tec eif code to control the interval in which a socket reconnection is attempted.
Reducing the retry interval from the default of 120 seconds to a much smaller value (I have had success using 5 seconds) will work around this problem.
To set this value add **RetryInterval=5** to rmad.conf
New TEC EIF libraries have provided a fix for this and have been included in FP 0003.

APAR IY47599 - Non-English support for wrmcdbclear
PROBLEM DESCRIPTION:

The wrmdbclear command is not working when output of wgetrim is in non-English language.
SOLUTION:

Defect 39805 - Wrmsendmsg throws a segmentation fault (TEC Defect 164498)
PROBLEM DESCRIPTION:
If a wrmsendmsg command is issued while RM server is down, when server has been started and the next wrmsendmsg is sent, this will cause a Segmentation Fault(coredump).
SOLUTION:
The root of this problem is in the TEC EIF library used to send events. The tec_put_event API form this library will seg fault if there are events cached when wrmsendmsg is started.
Note: wrmsend message does not fail if the cache is cleared befor execution.

3. Known Limitations and Workarounds

3.1 Fix pack installation issues for HP-UX

EXPLANATION: Installation order of HP-UX different from other platforms. Because support for the HP-UX platform was released in RM 4.1 patch 2, this patch 2 must be installed before installing RM 4.1 fix pack 3 on the HP-UX platform.

WORKAROUND: Run the full installation of Risk Manager for HP-UX, available from Risk Manager L2 support, before attempting to install this fix pack.

EXPLANATION: If the Tivoli Risk Manager Perl support is running when you install the fix pack on an HP-UX system, the installation will not be successful, and you will see the following error:

One or more errors occurred during copying of files (rmperl_hp_bin_files)

WORKAROUND: If you get this error, cancel the installation and stop Web IDS and Perl. After you have verified that Perl is not running, run the fix pack installation again.

3.2 Fix pack un-installation issues on HP-UX

EXPLANATION: After the fix pack has been installed and the uninstallation program is run on the HP-UX system, the uninstallation will complete successfully but not all of the Tivoli Risk Manager files will be removed.

WORKAROUND: Manually remove the files in the /opt/RISKMGR directory if you used the default installation directory after running the uninstallation program.

4. Documention Additions, Subtractions and/or Modifications

The information contained in this section should be considered additions to the IBM Tivoli Risk Manager publications. These additions will be added during the next product release of the IBM Tivoli Risk Manager library.

4.1 Using Sybase database on an HP-UX system with TEC and Risk Manager Archive Table

If you are planning to use a Sybase database on an HP-UX system with the Tivoli Enterprise Console and the Tivoli Risk Manager Archive Table, certain Sybase parameters will need to be changed during installation. During the installation of the Sybase server be sure to select UTF8 as the default character set instead of HP Roman 8.

After installing the Tivoli Enterprise Console and using the Tivoli Enterprise Console Database Assistant to create the Tivoli Enterprise Console database, do the following to disable the character set conversion:

1. Enter the isql utility using the sa account and password.

   isql -U sa -P sa password -S server

2. Run the following commands:

sp_configure "disable character set conversion", 1
go

3. Exit from the isql utility by using the exit command.
4. Stop and restart the Sybase server.

4.2 Customer ID attribute enablement (Included from Patch 01/02)

EXPLANATION: For background information on the customer ID attribute, refer to page 98 in the IBM Tivoli Risk Manager User's Guide, Version 4.1. For background information on how to customize incident rule, refer to pages 147 - 150 in the IBM Tivoli Risk Manager User's Guide, Version 4.1.

The following procedures document how to enable the customer ID attribute, and use it to correlate IBM Tivoli Risk Manager events.

PROCEDURES: To enable the event server to aggregate events using the customer ID attribute, rm_CustomerID, perform the following steps on each server:

1. Copy the following file to the RMADHOME/etc directory, where RMADHOME is the IBM Tivoli Risk Manager installation directory:

RMADHOME/etc/templates/provider_incident_rules.xml

2. Review the file to ensure that the threshold settings, and all other settings, are correct for your environment.

3. Edit the correlation engine RMA_conf file to activate the rules in the RMADHOME/etc/provider_incident_rules.xml file. To do this, add (or change) the file to include the following line:

rules=$RMADHOME/etc/provider_incident_rules.xml

4. Restart the agent to activate the changes you just made by entering the following command:

wrmadmin -r

After the provide_incident_rules.xml file has been updated and activated, the customer ID attribute must be set in the RM_SensorEvent events to fully enable incident creation on a per customer basis. Depending on the type of adapters deployed, there are several options for setting the customer ID attribute:

1. For logfile type adapters, the format (.fmt) file can be edited to include setting the attribute to the correct value - usually at the base level FORMAT.

2. For any adapter, an attribute map definition can be added to the correlation engine's RMA_conf file. This is accomplished by adding an entry to set the rm_CustomerID attribute. The agent must be restarted to activate this change.

3. For any adapter, edit the BAROC file and add a default setting for the rm_CustomerID attribute. At the Tivoli Enterprise Console server, this type of change should be activated by entering the following command:

rmcorr_cfg -update

4. For other event servers, restart the agent using the following command:

wrmadmin -r

5. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Websites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information that has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems

and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some easurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

5.1 Trademarks

IBM, the IBM logo, Tivoli, the Tivoli logo, AIX, NetView, Tivoli Enterprise, Tivoli Enterprise Console, and TME are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Lotus is a registered trademark of Lotus Development Corporation and International Business Machines Corporation in the United States or other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both. For a complete list of Intel trademarks, see http://www.intel.com/sites/corporate/tradmarx.htm.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.