o

IBM Tivoli Risk Manager
Version 4.2 Fix Pack 1
Readme File

Note:

Before using this information and the product it supports, read the information in Notices on page 32.

First Edition (September 2004)

This edition applies to IBM Tivoli Risk Manager, Version 4.2, fix pack 1 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

1 About this fix pack

This section provides general information about this fix pack. Read this entire document before you install this fix pack.

This readme document is provided in Adobe Acrobat format only.

For information about the localization pack that is provided with this fix pack, see the *Localization pack information* section of this readme file.

1.1 Fix pack contents

This fix pack provides the following contents:

- This readme file
- An image report for this fix pack
- The CD-ROM image of this fix pack

1.2 Patches superceded by this fix pack

The following patches are superceded by this fix pack:

- 4.2-RMG-0001LA
- 4.2-RMG-0002LA
- 4.2-RMG-0003LA
- 4.2-RMG-0004LA

1.3 Supported operating systems

The section lists the platforms and databases that are supported by this fix pack.

Supported operating system versions [1]	Roles				Optional components			
	Event server	Distributed correlation sever	Gateway	Client	Crystal Reports	Network IDS	Web IDS	Web application
AIX® 5L V5.1 (32-bit or 64-bit)	X	X	X	X		X[3]	X	X
AIX 5.L V5.2 (32-bit or 64-bit)	X	X	X	X		X[3]	X	X
Solaris® 8 (SPARC) [2]	X	X	X	X		X	X	X
Solaris 9 (SPARC)	X	X	X	X		X	X	X
HP-UX 11i (32-bit or 64-bit)	X	X	X	X			X	X
Windows® 2000 Professional (SP3)	X	X	X	X	X		X	X
Windows 2000 Server (SP3)	X	X	X	X	X		X	X
Windows 2000 Advanced Server (SP3)	X	X	X	X	X		X	X
Windows XP Professional		X	X	X	X		X	X
Windows 2003 Server	X	X	X	X	X		X	X
Red Hat Enterprise Linux AS 2.1 (IA32)	X	X	X	X		X	X	X

Supported operating system versions [1]	Roles				Optional components			
	Event server	Distributed correlation sever	Gateway	Client	Crystal Reports	Network IDS	Web IDS	Web application
Red Hat Enterprise Linux AS 3.0 (IA32)	X	X	X	X		X		
Red Hat Enterprise Linux ES 3.0 (IA32)	X	X	X	X		X		
SUSE LINUX Enterprise Server 8 (iA32)	X	X	X	X		X	X	X
SUSE LINUX Enterprise Server 8 (pSeries®)				X			X	
SUSE LINUX Enterprise Server 8 (zSeries®)	X	X	X	X		X	X	X
SUSE LINUX Enterprise Server 9 (iA32)	X	X	X	X		X		X

Operating system notes:

1. The information in this table is based on information available at the time of this fix pack. This table reflects those operating systems that have not reached end of life, as indicated by the operating system vendor. Refer to the online support from IBM for current support information.
2. Solaris refers to the Solaris Operating Environment and is hereinafter referred to as Solaris.
3. Network intrusion detection system (network IDS) is not supported on 64-bit systems.

RDBMS vendor	Version
IBM DB2®	7.2 (FP8), 8.1 (FP2)
Oracle	9i, 9i v2
Sybase	12
Microsoft SQL Server	7.0, 2000

1.4 New in this fix pack

The section provides information about changes that have been made to the Tivoli Risk Manager product.

- Support for managing queues is enhanced. Keywords are now provided that provide a means of controlling the size of queues and sending events about the queue status. For more information, see the Documentation updates section.
- Support for regular expressions is enhanced. A more robust and up-to-date version of the Xerces regular expression library is now used that provides broader support of standard regular expression syntax. For more information, see the Documentation updates section.
- Support for first failure data capture is added. For more information, see the Documentation updates section.
- The msg attribute included in the RMAgent_Inactive event has been enhanced to include the hostname and IP address of the agent which is no longer sending RMAgent_HeartBeat events. For more information, see the Documentation updates section.
- Support for Windows 2003 Server is now provided.

2 Installation and configuration

2.1 Prerequisites

The following software is required for Tivoli Risk Manger fix pack 1:

- IBM Tivoli Risk Manager, Version 4.2
- IBM Tivoli Enterprise Console, Version 3.9 with FP01 (For the event server role only.)
- For Red Hat Enterprise Linux, the recommended version of the Java run time is the IBM JRE 1.3.1-6 or later. If you cannot use these versions, contact IBM software support.

2.2 Installation notes

This section provides additional information about installing the Tivoli Risk Manager product.

- If you installed the Tivoli Risk Manager 4.2.0-RMG-FP01fix pack and want to install an optional component (for example, Crystal Reports) that was not installed during the initial installation of the Tivoli Risk Manager product, contact IBM Software Support for the installation fix pack that is required to perform this procedure.
- This fix pack can be installed either as a full installation or a patch. For more information about determining which method you should use, see the Installation instructions section.
- The Windows event monitor creates registry keys to mark the last place the Windows event logs were read. These entries are used to determine where to start reading when the event monitor or the Tivoli Risk Manager agent is restarted. When the Tivoli Risk Manager product is uninstalled, the uninstaller does not remove these registry keys from the registry. If you reinstall the event monitor, the old registry keys are used the next time event monitor is started, and the event monitor starts reading old events.
  To ensure that the Windows event monitor starts reading from the current date only, and does not read older events, delete the following event monitor registry key before starting the event monitor for the first time: HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Riskmgr\Agent\RMLogfile
- The installation of the Tivoli Risk Manager Web application component on a Solaris system might be very slow or stop. The default maximum number of open files might be set too low for the WebSphere application server to successfully install the Tivoli Web application component. This causes the WebSphere application server to continually retry the installation rather than returning an error code.
  You can determine the file descriptor limit by issuing the following command:

  ulimit -n

  To successfully install the Tivoli Risk Manager Web application component on the WebSphere application server, it must be started with a maximum file descriptor of no less than 1024 (assuming that the sample WebSphere application server applications are installed with the Tivoli Enterprise Console Web application), prior to installing the Tivoli Risk Manager Web application using one of the following procedures. Before you do this, however, you should read the Solaris documentation to understand the precautions, execution, and ramifications of making these changes. The exact value of the maximum file descriptor might need to change depending on how many WebSphere application server applications are installed.

  Use one of the following methods to change the maximum file descriptor:

  1. Stop the WebSphere application server.
  2. Issue the following command:
     ulimit -n 1024
  3. Restart the WebSphere application server from the same command session from which the **ulimit** command was issued.
  4. Install the Tivoli Risk Manager product.

A more permanent solution is to change the system values for file descriptors by setting the following attributes in the /etc/system file:

```
rlim_fd_cur
rlim_fd_max
```

- For a new installation of the Tivoli Risk Manager product with a Sybase database, the Tivoli Risk Manager table is installed in the default segment of the Tivoli Enterprise Console product database. The default segment that is defined by the Tivoli Enterprise Console installation is very small, and it holds only a very limited number of Tivoli Risk Manager archive table events. To use the Tivoli Risk Manager product with the default implementation on Sybase, the default segment in the Tivoli Enterprise Console database can be increased by adding another device.

  The following procedure provides an example of how to increase the default segment size by creating a 200 MB device in the default segment called TEC_SYSTEM_2.

  Notes:
  - The ALTER DATABASE statement automatically adds the new device to the default segment.
  - Use the user ID for the Sybase system to set up the Sybase environment to perform this procedure. This user ID must have the appropriate authority and Sybase environment.

  1. Create a script named rm_exp_archive_table.syb.sql file as follows:

     ```
     use master
     go
     DISK INIT name="TEC_SYSTEM_2",
     physname="/data/sybase/data/TEC_SYSTEM_2",
     vdevno=14,
     size=102400
     go
     ALTER DATABASE tec
     on TEC_SYSTEM_2 = 200
     go
     ```

  2. Evaluate the following parameters and change them to meet the needs of your installation:
     - **DISK INIT** name: choose a name that is appropriate for your installation.
     - **physname**: specify the operating system path name to the device you are creating.
     - **vdevno**: ensure this is an unused number. Use the following command to determine which numbers are currently used: select distinct low/16777216 from sysdevices
  3. Issue the following command to run the script:

     ```
     isql -Usa -P<pw> -S<system> -i rm_exp_archive_table.syb.sql
     ```

     The variable <*pw*> is the SQL password and the variable <*system*> is the name of the system that the database is installed on.

- The following message is displayed during installation to indicate that the Java executable cannot be found:

  ```
  "JVM not found"
  ```

  This can be caused by having insufficient space available on the file system that contains the temporary directory. If this is the reason, you can do one of the following:

  - Free space in that file system
  - Allocate more space to the file system

  The space that is required can be up to three times the size of the installed Java JRE.

- If you reinstall the Tivoli Risk Manager product and change the transport type to TME, change the value of the **TMEEndpoint** keyword to true in the /etc/Tivoli/rma_eif_env.sh script file as follows:

  ```
  TMEEndpoint=true
  ```

2.3 Installation instructions

This section provides information about installing this fix pack.

The Tivoli Risk Manager 4.2.0-RMG-FP01 fix pack can be installed either as a full installation or a patch installation. The full installation must be performed under the following conditions:

- You are using the Web application with any RDBMS product other than DB2.
- You are installing this fix pack on one of the following platforms:

  Windows 2003 Server
  Red Hat Enterprise Linux AS 3.0
  Red Hat Enterprise Linux ES 3.0
  SUSE LINUX Enterprise Server 8 (iA32)
  SUSE LINUX Enterprise Server 9 (iA32)

Contact IBM Software Support for the installation package you must use for a full installation.

2.3.1 Patch installation

Issue the following command to install the patch:

rm4201_setup_<*platform*> [-silent | -console]

For <*platform*>, specify one of the following platforms:

aix:	AIX versions supported by the Tivoli Risk Manager product
hpux:	HP-UX versions supported by the Tivoli Risk Manager product
linux:	Linux (IA32) versions supported by the Tivoli Risk Manager product
linuxppc:	Linux (PPC) versions supported by the Tivoli Risk Manager product
solaris:	Solaris (SPARC) versions supported by the Tivoli Risk Manager product
win:	Windows versions supported by the Tivoli Risk Manager product

You can specify one of the following options:

-silent	This option requires no user input. Check the log file in the installation directory for a non-zero return code to determine whether the installation is successful.
-console	This option provides a terminal (text-mode) installation. Note that this option is not available on Windows platforms.

If you do not specify an option, the following windows are displayed:

- Language
- Welcome
- Pre-installation
- Post-installation

No user input is required for these windows. Click **Next** when each window is displayed.

If you installed this fix pack on the event server, perform the following procedure after you finish the installation:

1. Ensure that the rule base that you want to use is the current rule base.
2. Issue the following command:
   rmcorr_cfg -update

   Note: This command updates the rule base. It also stops and restarts the Tivoli Enterprise Console event server.

2.4 Localization pack information

The localization packs that are included with the 4.2-RMG-FP01 fix pack contain updated translations for all languages supported by the Tivoli Risk Manager, Version 4.2 product. This section provides the following localization pack information:

- Localization pack notes
- Localization pack installation instructions

2.4.1 Localization pack notes

Review the information in this section before you install the 4.2-RMG-FP01 fix pack.

- The updated international language resources included in this fix pack reflect changes in the Tivoli Risk Manager user interface and messages.
- The differences between a full installation and a patch installation are the number of files installed and the prerequisite checks performed prior to installation.
- The windows that are displayed during a patch installation are the same as during a full installation.

2.4.2 Localization pack installation instructions

This section provides localization pack installation information. Localization packs for the Tivoli Risk Manager, Version 4.2 fix pack 01 can be installed either as a full installation or as a patch installation. Use the full installation when you perform a full installation of the base product (For more information, refer to the Installation instructions section above.) Use the patch installation when you perform a patch installation of the base product.

2.4.2.1 Full installation

To perform a full installation of international language resources, see the installation instructions in the International Language Support section of the *IBM Tivoli Risk Manager Release Notes*, Version 4.2.

2.4.2.2 Patch installation

To perform a patch installation, issue one of the following commands:

For Windows platforms:

```
rmlp4201_setupwin32.exe
```

For UNIX and Linux platforms:

```
./rmlp4201_setup<platform>.bin
```

For <*platform*>, specify one of the following platforms:

aix:	AIX versions supported by the Tivoli Risk Manager product
hp11x:	HP-UX versions supported by the Tivoli Risk Manager product
linux:	Linux (IA32) versions supported by the Tivoli Risk Manager product
linuxppc:	Linux (PPC) versions supported by the Tivoli Risk Manager product
solaris:	Solaris (SPARC) versions supported by the Tivoli Risk Manager product

For Linux for zSeries (S/390):

```
java -Dis.javahome=/opt/IBMJava2-s390-131/jre -cp ./rmlp4201_setup.jar run
```

3 APARs corrected by this fix pack

This section provides a description and the resolution of the APAR fixes that are provide by the 4.2.0-RMG-FP01 fix pack.

APAR: IY48016

Symptom: When multiple instances of the Web intrusion detection system (Web IDS) are running on the same system, the resume function does not function correctly because all instances are using the same copy of the webids.lastread file.

Resolution: Each instance of the Web IDS function now uses its own copy of the webids.lastread file.

APAR: IY50483

Symptom: On a Tivoli Risk Manager or Tivoli Enterprise Console server, the tec_rule process exhibits extensive CPU utilization. This causes incoming events to remain in the QUEUED state.

Resolution: The Tivoli Risk Manager Tivoli Enterprise Console rules for generating incident groups have been modified to improve performance. Additional configuration options for incident group processing have been added to the riskmgr_config.pro file in the $RMADHOME/etc/tec/rules directory. For more information about using these options, see the comments in the riskmgr_config.pro file.

APAR: IY52322

Symptom: The distributed correlation server stops when a partial event is received.

Resolution: A new Tivoli Enterprise Console API keyword, **ReadRetryInterval**, is used to configure the timeout value that is used by the Event Integration Facility API when a partial event is received.

The default value for this keyword is 120 seconds.

When the Event Integration Facility sender works with events that are larger than 2 KB, it divides the event into two packets that are delivered using the socket connection. If the receiver determines that the event is a partial event, it waits for the period of time that is specified by this keyword before it retrieves the second packet and completes the process. If the second packet is not received during this period of time, the partial event that was received is discarded and a message is written to the log.

APAR: IY52323

Symptom: Unused socket connections between Tivoli Risk Manager agents are not closed when a system is restarted.

Resolution: Unused socket connections between agents are now automatically closed.

APAR IY53525

Symptom: On UNIX systems, the event monitor does not read from a new log file that is created when the log file is rotated.

Resolution: The event monitor now correctly reads from new log files.

APAR IY53527

Symptom: Documentation is required for the regular expression syntax supported by the event monitor.

Resolution: Support for regular expressions has been improved and documentation is provided. For the documentation changes, see the Documentation updates section.

APAR: IY53678

Symptom: The event monitor generates a Java null pointer exception when it parses events that match the index pattern for a class, but not the class pattern defined for that class in the XML file.

Resolution: Event monitor processing is changed so that if an event string matches the index pattern for a class, but not the class pattern, it is not considered a match for that class and it continues to search for another matching class.

APAR: IY53713

Symptom: A duplicate key exception is received when a group of events is inserted into the database and the insertion is only partially successful.

Resolution: The insertion of events into the database is now done correctly. Each event is inserted only once. If a duplicate key is detected, processing has been enhanced to discard the duplicate event.

APAR: IY54408

Symptom: Repeated use of the **wrmadmin -i** command causes the system to stop, because the system runs out of memory.

Resolution: The **wrmadmin -i** command can now be used repeatedly without causing system memory problems.

APAR: IY54568

Symptom: The Windows event log event monitor reprocesses events that it already processed.

Resolution: Events are not repeatedly reprocessed.

APAR: IY55241

Symptom: The network IDS files should be updated to include the correct signatures for the CAN-2002-0562 vulnerability.

Resolution: The signature file is updated to include the correct signatures.

APAR: IY55319

Symptom: The **wrmqueue** command does not complete when a large number of events are being queued.

Resolution: Internal processes related to the **wrmqueue** command are changed to correct this problem. For more information about this command, see the Documentation updates section.

APAR IY55895

Symptom: The *IBM Tivoli Risk Manager Adapters Guide* and other PDF documents supplied with various adapter packages reference the Event Mapping Table. This table is not posted on the Web site and is not available for download or reference.

Resolution: The Event Mapping Table document (DCF 1171204) is now posted on the Risk Manager support Web site: http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliRiskManager.html.

APAR IY55927

Symptom: When running in a DBCS locale, the Tivoli Risk Manager agent discards events that contain DBCS characters. The following message is written in the Tivoli Risk Manager message log:

HRMAG0135W An event integration facility TECAgent filtered the following event

Resolution: The Tivoli Risk Manager agent now correctly processes events that contain DBCS characters.

APAR: IY56431

Symptom: The Tivoli Risk Manager event repository does not support Microsoft SQL if it was installed with the case sensitive option. The following symptoms indicate that this problem exists:

- Events are not written to the Microsoft SQL event archive.
- The following error message is written in the Tivoli Risk Manager message log:

  HRMAG0082E SQL exception:[Microsoft] [SQLServer 2000 Driver for JDBC]

  [SQLServer]Invalid object name 'RM_T_ARC41'

Resolution: Issue the following command to run the DDL file that corrects this problem:

```
osql -U tec -P <password> -d tec -S <server> -n -i %RMADHOME%\dbschema\rm_t_arc41_uc.ms.sql
```

4 Known limitations

This section provides a description of each limitation and a workaround if one is available.

4.1 Installation

Limitation: The following incorrect warning message is displayed during installation:

WARNING: could not copy log output /opt/RISKMGR/rminstall_log.txt

(No such file or directory)

Workaround: If you suspect that errors occurred during the installation, reinstall the Tivoli Risk Manager product and specify the following option on the installation command to create the log in a directory other than /opt/RISKMGR:

-l !<*fully qualified path*>

The variable <*fully qualified path*> is the fully qualified path of the rminstall_log.txt file.

4.2 Correlation server

Limitation: The Tivoli Risk Manager agent events (for example RM_Sensor, RM_Error, RMAgent_Inactive, and RMAgent_QueueProblem) are not sent to the Tivoli Enterprise Console product and are not displayed on the event console. This problem applies only to systems that meet *both* of the following criteria:

- Your installation is either an event server or distributed correlation server installation
- You did not perform a default installation. Instead, you selected to only send incident events (RM_Incident) to the Tivoli Enterprise Console server. For more information about installation choices, see pages 102 and 114 of the *Tivoli Risk Manager Installation Guide*, Version 4.2.

Workaround: To resolve this problem, use the following procedure

1. Edit the $RMADHOME/etc/rmagent.xml file on your correlation and event servers and add the following filter definition:

```
<filter name = "nonSensorEvents">
    <OR>
        <isa value = "RM_AgentProblem"/>
        <NOT>
        <isa value = "RM_SensorEvent"/>
        </NOT>
     </OR>
  </filter>
```

2. Change the existing connector definition by modifying the <withfilter name ="incidents"/> statement to specify the new filter name nonSensorEvents as follows:

```
<connector>
    <from name ="correlation"/>
    <to name ="incident_sender"/>
    <withfilter name ="nonSensorEvents"/>
  </connector>
```

3. Restart the agent for the changes to take effect.

4.3 Tivoli Enterprise Console event server

Limitation: Once RMAgent_Inactive and RMAgent_QueueProblem events are sent to the event console, they are displayed in the RM_SensorEvent group view intermingled with other sensor events. If you deployed the default configuration for your Tivoli event console or distributed correlation servers, the RM_SensorEvent group view might contain many events. This makes it difficult to recognize the Tivoli Risk Manager agent events that are warning you about Tivoli Risk Manager agent and queue problems in your network.

Workaround: To make it easier to monitor agent problems, use the following procedure to customize the RM_Error group view in the event console to include RMAgent_Inactive and RMAgent_QueueProblem events:

1. From the main event console view, click **Windows → Configuration**.
2. In the left pane, click **Event Groups**.
3. Click **RM_Error**.
4. Right click the window and click **Create Filter**. The Add Event Group Filter window is displayed.
5. In the Name field, type RM_AgentProblem.
6. In the Description field, type an optional description of the filter.
7. Click **Add Constraint**.
8. Select **Class** from the attribute list.
9. Select **Like** from the operator list.
10. Type RMAgent_% for the value. (This value is case sensitive.)
11. Click **OK**.
12. From the Add Event Group Filter window, click **Test SQL** to determine if the filter produces the correct number of events.
13. Click **OK** to save the changes.
14. Stop and restart the event console.
15. Click **Windows → Summary Chart View** and open the RM_Error console group to determine if the filter functioned correctly.

4.4 Tivoli Risk Manager agent

- Limitation: Memory constraints can cause out of memory problems. This problem is most apparent on AIX systems. This can happen when the number of receivers or senders is increased, or the **instanceCount** parameter is added to any rmagent.xml destination definition. This problem can also occur on other platforms if you add a large number of senders or a large number of **instanceCounts**, because both options create additional threads and increase memory usage.

  The Tivoli Risk Manager agent is a Java process, and is constrained by the memory allocations of the Java environment. On AIX, this memory limit is significantly affected by the low default values for storage allocations in the /etc/security/limits file. To enable Tivoli Risk Manager to run in a default AIX installation, the maximum Java storage was intentionally limited by the **RmagentMemMax** parameter, which is defined in the RMADHOME/etc/rmad.conf file. On AIX, this value is set to 92 MB, which provides only enough memory allocation for a basic server installation.

  Workaround: The **RmagentMemMax** parameter can be used on any platform to increase the maximum memory available to Tivoli Risk Manager. For example, on AIX, perform the following procedure:

  1. Increase the default values for the data,rss and stack values in the limits file (or use the **ulimit** command)
  2. Increase the RmagentMemMax value in the rmad.conf file.
  3. Log off and then log on the system.
  4. Issue the **wrmadmin -r** command to restart the Tivoli Risk Manager agent.

- Limitation: The Tivoli Risk Manager product cannot be restarted if the disk where the persistence directory is located is full.

  Workaround: Ensure that there is enough free disk space before restarting the Tivoli Risk Manager product. Use the following formula to determine the amount of disk space that is needed:

(1 + number of destinations) x 20 MB

The *number of destinations* is the number of destinations that is defined in the rmagent.xml file.

- Limitation: If the first character of an event attribute is a single quotation mark, the event is corrupted because the single quotation mark and last character of the event attribute is removed. The following example shows a leading quotation mark specified for the msg event attribute and the result:

  'myHostname' is acting suspiciously

  The corresponding MSG column in the archive table will contain the following:

  myHostname' is acting suspiciousl

  Workaround: Avoid using leading single quotation marks in event attributes if possible. Otherwise, there is no workaround available.

4.5 DNS resolution

Limitation: For Solaris, the **wrmdns** command does not start DNS resolution.

Workaround: Do the following procedure to start DNS resolution:

1. Edit the summary_engine.conf file and the incident_engine.conf file.
2. Change the dnsResolver=off entry in both files to dnsResolver=on.
3. Issue the following command to restart the Tivoli Risk Manager agent:
   wrmadmin -r

4.6 Message and trace logging

- Limitation: You might not be able to dynamically change trace and log level settings on some Linux systems, because Linux default IP filtering and firewall protection is very restrictive.

  The JLog package included with the Tivoli Risk Manager product provides the ability to change trace and log settings dynamically while the Tivoli Risk Manager agent is running. For more information about this function, see the Logging Command Line Interface section of the *IBM Tivoli Risk Manager Problem Determination Guide*.

  When the Tivoli Risk Manager agent starts, it calls the JLog Log Manager which creates a log command server that listens on port 9992. The **logcmd** client program communicates with the log command server over this port. On some Linux systems, port 9992 is not listening when the Tivoli Risk Manager agent is running and the **logcmd** commands fail with a Java ConnectionException. This is caused by IP filter and firewall protection that is installed. If one of the following programs are installed on your Linux system and you are unable to see port 9992 LISTENING when the Tivoli Risk Manager agent starts, the IP firewall is preventing the port from being accessed:

  - lokkit
  - ipchains
  - iptables
  - ipfwadm

  Workaround: Refer to your Linux system documentation for the procedure to unlock port 9992. If you want to leave the port locked for security reasons, there is no interference with the standard Tivoli Risk Manager agent logging, except that you cannot dynamically change trace settings.

- Limitation: On UNIX systems, log files are compressed when they are rotated and this makes them unreadable by the host IDS adapter.

  Workaround: To prevent this problem, turn off the log compression function for the most recently rotated log file.

- Limitation: The following message (HRMAG0147I) does not always immediately follow the repeated message:

The previous message was repeated {n} times

In this case there is no way to determine which message was repeated.

Workaround: No workaround is available.

4.7 Network IDS component

Limitation: When starting the Network IDS component on 32-bit AIX systems, the component might not start. This can occur because the /dev/bpf0 device that is needed by the Network IDS component to monitor the network is not defined, or it has not started correctly since the system was last rebooted.

Workaround: Reset or define the /dev/bpf0 device using the following procedure:

1. From an AIX terminal session, issue the **tcpdump** command.
2. Press Ctrl+c to terminate the **tcpdump** command after the following message is displayed to indicate that the Ethernet connection has been started:

   listening on *xxx*

   The letters *xxx* represent the Ethernet device number, for example, en0.
3. Issue the following commands to stop and restart the Network IDS process:

   stopnids

   startnids

4.8 Web IDS component

- Limitation: Disabling log file rollover for the Web IDS component by coding fileMatch_value=0 in the webids.cfg file causes an error message to be displayed.

  Workaround: There is no workaround for this problem. Log file rollover cannot be disabled.
- Limitation: The Web IDS component loops if it is configured to monitor multiple Web servers on the same system and the access logs for the servers are all in the same directory.

  Workaround: Store the Web server access logs in different directories.
- Limitation: The **webids -d** command does not write debugging information to standard output (STDOUT). For more information, see the Documentation updates section.

  Workaround: No workaround is available.

4.9 Web application

- Limitation (APAR IY58098): If the system you are running the Java console on is not on the local subnet where the WebSphere application server is running, you might be unable to log on to the Tivoli Risk Manager Web console. This is because the rmweb.pl script is updated with the short hostname instead of the fully qualified hostname of the system running the Web application server when the Tivoli Risk Manager Web application is installed.

  Workaround: Perform the following procedure to specify the fully qualified hostname of the Web application server:

  1. Edit the **rmweb.pl** script and located in directory RMADHOME/cgi-bin of the event server.
  2. Locate the following line (approximately line 47):

     ```
     $output .= "METHOD=POST ACTION=\"http://server1:9080/rmwebapp42/logon\">');\n";
     ```

  3. Change the short hostname in the URL string to a fully qualified hostname, (for example, server1.mycompany.com.
- Limitation: If you have an outdated version of Mozilla installed, you might not be able to use the Web application.

Workaround: Install Mozilla version 1.7.2 or later.

- Limitation: After uninstalling the Tivoli Risk Manager Web application, the Tivoli Risk Manager JDBC provider still exists as a WebSphere application server resource.

  Workaround: Use the following procedure to remove the Tivoli Risk Manager JDBC provider:

  1. Log on to the WebSphere Application Server administrator's console as an administrator.
  2. Click **Resources**.
  3. Click **JDBC Providers**.
  4. Ensure the scope is set to the server level.
  5. Select the **Risk Manager JDBC Provider** check box.
  6. Click **Delete**.

- Limitation: The online help has an incorrect reference to help for adapter addresses. When you click the question mark (?) from the System Addresses window, the help panel displays the following selections to obtain system information:

  Source Address
  Destination Address
  Sensor Address
  Adapter Address
  Other

  Workaround: There is no workaround. Information for the Adapter Address is not available.

5 Documentation updates

This section provides a description of the documentation updates for to the Tivoli Risk Manager, Version 4.2 library. Read the information in the following sections to understand the corrections that should be made to the library and to understand functional improvements that have been made to the Tivoli Risk Manager product:

- Miscellaneous documentation updates
- Queue management and operation
- FFDC and other trace documentation
- Regular expression support

5.1 Miscellaneous documentation corrections

This section provides information about miscellaneous documentation corrections that should be made to the Tivoli Risk Manager library and documentation of minor functional changes that have been made for this fix pack.

5.1.1 IBM Tivoli Risk Manager Administrator's Guide

- The following text should be added to the Customizing Incident-Based Correlation Rules section on page 101:

The <threshold> and <aggregate> elements of the rule determine when to generate an incident. The default rules that are provided with the Tivoli Risk Manager product aggregate events by accumulating the **rm_Level** value of each sensor event until the **thresholdCount** value is reached, at which point an incident is generated. The **rm_Level** value represents the relative weight, or severity, of each event. An alternate method is to count the number of events, and generate an incident when the count reaches a particular threshold count. To enable counting events, remove the <aggregate> element from the rule and adjust the **thresholdCount** parameter to represent the number of events necessary to generate an incident.

The **attributeSet** parameter in the <cloneable> element of the rule determines which attributes from the event are used to aggregate incoming events as candidates for a possible incident. The three standard correlation attributes that are used in this parameter are any combination of **rm_SourceToken**, **rm_DestinationToken** and **rm_CategoryToken** attributes. The following is a list of available attributes names that can be specified in the **attributeSet** parameter. Unless otherwise noted, the attribute name used in the rule is the same as the attribute name from the incoming events.

- rm_SensorToken
- rm_SourceToken
- rm_DestinationToken
- rm_CategoryToken (synonym for rm_ClassCategory)
- rm_CategoryDescription (synonym for rm_ClassCategoryDescription)
- rm_CustomerID
- rm_Signature
- rm_Timestamp32
- rm_Level

- The following change should be made to the Setting an Attribute to a Specific Value section on page 103:

The <parameters> element in the <action> element of a rule can be used to change the value of any RM_Incident event attribute, with the exception of the hostname and msg attributes.

The second example on page 103 assigns the msg attribute; this example is incorrect and should be deleted.

- The first paragraph of the Resource IDs and Dynamic Data section on page 125 should be changed as follows:

Resource IDs and Dynamic Data: The text displayed in these regions is either specified by hard coded text or a resource ID.

Hard coding the text is an easier way to code the text, because you only have to update one file and you do not have to stop and restart the WebSphere product for the changes to take affect. Note that is you are using the Tivoli Risk Manager product with a localization pack, you should use the resource ID method.

To use hard coded text, begin and end the text string with &quot.. Use the following procedure to hard code the text.

1. Edit the AdvisorRules.xml file.
2. Add the following line to the file:

   title="&quot.View CVE Recommendation &quot."
3. Save the AdvisorRules.xml file.

When the Web page is displayed, *View CVE Recommendations* is displayed in the title area.

You can also use dynamic data within hard coded text by coding a variable in the string that specifies an event or incident attribute. For example, to display the rm_Category attribute value within hard coded text, the text in step 2 would be coded as follows:

title="&quot.View Recommendations for &rm_Category Event &quot."

The remainder of the Resource IDs and Dynamic Data section on page 125 is unchanged. Review this information to learn more about dynamic data and using resource IDs.

- The Filtering Attributes section on page 47, should be changed as follows:

  ### Filtering Attributes

  You can filter your attributes so they are not sent to the Tivoli Enterprise Console server.

  You can add a configuration option to the eif_sender.conf file at your agent and distributed correlation server to not send some extended slots to the Tivoli Enterprise Console server.

  For example, add the following line to eif_sender.conf:

  filterAttributes=/opt/RISKMGR/etc/templates/sensorevent_attributeFilter.xml

  For an example of this filtering, see the RMADHOME /etc/templates/sensorevent_attributeFilter.xml file.

- The following keyword should be documented in Appendix A, Event Integration Facility Sender and Receiver Keywords:

  filterAttributes=pathname ...

  Specifies the full path name of one or more XML files that contain attribute filtering specifications. The specifications can be used to filter out extended attributes from the event before it is transmitted. Attribute filtering is useful for an Event Integration Facility sender subcomponent that is sending events to a Tivoli Event Console server, to eliminate unnecessary network traffic and improve performance.

  For a sample attribute filtering specification file, see the following file:

  RMADHOME /etc/templates/sensorevent_attributeFilter.xml

  ReadRetryInterval=seconds

  Specifies the number of seconds the Event Integration Facility receiver waits when a partial event is received. If the receiver determines that the event is a partial event, it waits for the period of time that is specified by this keyword before it retrieves the second packet and completes the process. If the second packet is not received during this period of time, the partial event that was received is discarded and a message is written to the log. The default value is 120 seconds.

- The Manually Configuring the Event Monitor section on page 192 provides an incorrect example in step 3. The lines that have <source name="monitor_receiver_webids" should be changed to <source name="monitor_receiver_nids" as follows:

```
<!-- Event Monitor for NIDS -->
<source name="monitor_receiver_nids"
class="com.tivoli.RiskManager.Agent.Transports.Receivers.rmaMonitorReceiver">
<set key="RMA_conf" value="/opt/RISKMGR/etc/monitor_receiver_nids.conf"/>
</source>
```

- The Heartbeat Monitoring section on page 87 should be changed as follows:

  Tivoli Risk Manager self-monitors the agents deployed in your network and warns you when an agent becomes inactive. The warning is an RMAgent_Inactive event generated at one of your correlation servers. RMAgent_Inactive events are included in the Tivoli Enterprise Console database and viewed on the console. The following warning message is displayed:

  Missing heartbeat for agent: <*hostname*>/<*ip address*>

  The <*hostname*> and <*ip address*> are the host name and IP address values for the agent which is no longer sending RMAgent_HeartBeat events.

  By default, each agent is configured to generate RMAgent_HeartBeat events. Each correlation server is configured to monitor the RMAgent_HeartBeat events and generate RMAgent_Inactive events when an agent stops sending regular RMAgent_HeartBeat events. By default, there will be an RM_Sensor event created to represent each agent that generates RMAgent_HeartBeat events. The RMAgent_HeartBeat events are not typically forwarded to your Tivoli Enterprise Console server or database.

5.1.2 IBM Tivoli Risk Manager Command Reference

It is incorrectly stated on page 25 that you can use the **webids -d** command to write debugging information to standard output (STDOUT), which you can then redirect to another file. This option does not function correctly and should not be used.

5.1.3 IBM Tivoli Risk Manager Installation Guide

Appendix E, Removing Components, should be updated to include the following information:

Perform the following tasks before you uninstall Tivoli Risk Manager components:

1. Shut down all Tivoli Risk Manager adapters.
2. Issue the **wrmadmin -k** command to shut down the Tivoli Risk Manager product.
3. If you are removing the event server, perform the following tasks:
   a. Issue one of the following commands:
      For UNIX: **rmcorr_cfg -delete**

      For Windows: **bash rmcorr_cfg -delete**

      Note: This command does the following:

      - This command loads the default rule base. To use a customized rule base, manually load it using the GUI or the **wrb** command to load it manually.
      - Stops and restarts the Tivoli Enterprise Console event server

   b. Issue the **wrmadmin -k** command.
4. Uninstall the component. For information about the command you should use for the component you are removing, see Table 11 on page 177.

Notes:

1. Tivoli Risk Manager files that have been changed or adapter files that have been added are not removed from the Tivoli Risk Manager directory.

2. On the event server, the Tivoli Risk Manager archive table, database views, and event console event groups are not removed during uninstallation. If you want to remove these components, you must remove them manually.

5.1.4 IBM Tivoli Risk Manager Problem Determination Guide

The following information should be added to the Tivoli Management Environment Send Connection Type section on page 23:

If the transport type was changed to TME when the Tivoli Risk Manager product was reinstalled, the value of the TMEEndpoint keyword must be changed to true in the /etc/Tivoli/rma_eif_env.sh script file as follows:

```
TMEEndpoint=true
```

5.2 Queue management and operation

This section provides information about enhancements that have been made to the operation and management of queues for APAR IY55319. The changes have been made to improve the management of disk space that is used by persistent queues. Prior to this change, if events were placed on a queue faster than they were processed for an extended period of time, the Tivoli Risk Manager product failed and the administrator was not informed of the reason. To resolve this problem, configuration parameters have been added to manage the queues and to inform administrators about the status of the queues. For more information about these changes, review the following changes to the Queues and Event Persistence section of the *IBM Tivoli Risk Manager Administrator's Guide*:

Queues and Event Persistence

Each subcomponent of the agent that is referenced in the rmagent.xml file as a to setting in a connector has a queue associated with its processing. Events that the subcomponent needs to process are put on the associated queue by the subcomponent specified as the from setting in the connector. The processing subcomponent removes the events from the queue when it is ready to process events.

Understanding Persistence

Persistence is controlled by the **persist** parameter in the rmagent.xml file. By default, the events are persisted to disk when they are placed on a queue. When the processing subcomponent completes its task, the event is removed from disk. You can configure both engine and destination component queues to not persist events to a disk. Review the following information carefully before you determine whether you want to persist events.

The following table provides information to help you understand event persistence:

Description	Persistence	No persistence
All events are written to disk	Yes	No
Failed events are written to disk	Yes	Yes
Queued events are written to disk (as failed retry events) when the agent is stopped	No	Yes
Failed (retry) events are processed when the agent is started	Yes	Yes
Failed (permanent) events are written to disk	Yes	Yes

Why would you turn off persistence?

The processing might be faster since you bypass writing event data to disk and removing it later.

Why would you NOT turn off persistence?

Your system does not have unlimited memory available to the agent. If the events are not persisted to disk, they must be maintained in memory. You do not want to lose events if an unexpected error condition causes the agent to terminate. With persistence off, you might lose event data.

Should you turn off persistence?

The option to turn off persistence is deprecated. You are strongly encouraged to use persistence.

To turn off persistence, edit the rmagent.xml file and add persist="no" to the subcomponent definition, for example:

```
<destination name="eif_sender"
        class="com.tivoli.RiskManager.Agent.Transports.Senders.rmaEifSender"
        persist="no" >
</destination>
```

Queue management and control parameters

The following optional parameters can be used with the <destination> element in the rmagent.xml configuration file to control the operation and management of the queue:

- **persist**
- **queueMaxSize**
- **queueThresholdSize**
- **queueMessageInterval**
- **errorRoute**

The size of the queue and the amount of free disk space are evaluated when events are to be queued. If the size of the queue approaches the size specified by the **queueMaxSize** and **queueThresholdSize** parameters, an RMAgent_QueueProblem event is sent to the event console specified by the **errorRoute** parameter. The **queueMessageInterval** parameter controls how often the queue warning events are sent. If no events are to be queued or the queue is already in one of the Waiting states, the queue size and disk space are not evaluated and no queue warning events will be generated.

The following information provides a description of each parameter:

queueThresholdSize

- This parameter specifies the size that the queue must reach before a queue warning event is sent to the event console. The first event is sent when this value is initially reached and additional events are sent again at time intervals specified by the **queueMessageInterval** parameter to the event console that is specified by the **errorRoute** parameter.
- If a queue reaches the size specified by this parameter, it does not stop processing events for that subcomponent.
- The value of this parameter can be an integer between 0 and 2147483647. The default value 0 indicates that there is no size limit.
- When a queue is in this state, its status is Running(THRESHOLD) as displayed by the **wrmqueue -l** command.

queueMaxSize

- This parameter specifies the maximum number of events that the queue can contain. When the number of events in the queue approaches value, the component that is sending events to the queue stops processing and a queue warning event is sent to the event console. The first event is sent when this value is initially reached and additional events are sent again at time intervals specified by the **queueMessageInterval** parameter to the event console that is specified by the **errorRoute** parameter. The default interval is 15 minutes.
- The value of this parameter can be an integer between 0 and 2147483647. The default value 0 indicates that there is no size limit. The value of this parameter must be greater than the **queueThresholdsize** parameter value.
- When a queue reaches the maximum size, its status is Waiting(MAX) as displayed by the **wrmqueue -l** command.

queueMessageInterval

- This parameter specifies the time (in milliseconds) before the next RMAgent_QueueProblem queue warning event is sent. Use this parameter to limit the number of queue warning events that are sent when the queue has exceeded the size specified by either the **queueMaxSize** or **queueThresholdSize** parameters.
- The default value is 900000 (15 minutes).

errorRoute

- This parameter specifies the component (typically an event console) that queue warning events are sent to when either the **queueMaxSize** or **queueThresholdSize** parameter values are exceeded.
- The queue warning events are queued with all other events for this route. Use this parameter to expedite sending the queue warning events by defining a separate destination address for the error route. This will ensure the delivery of the queue warning event in a timely manner.
- Multiple error routes can be defined. RMAgent_QueueProblem queue warning events are sent to all specified error routes.
- There is no default error route. If this parameter is not specified, no RMAgent_QueueProblem queue warning events are sent.

Example of using queue management and control parameters

This section provides an example of using the queue management and control parameters based on the following scenario:

Goals	Parameter used	Example
Ensure that the number of queued events never exceeds 100 000.	queueMaxSize	queueMaxSize = "100000"
You want a queue warning event sent when the number of queued events reaches 10 000	queueThresholdSize	queueThresholdSize="10000"
You want a queue warning event sent.	errorRoute	See below for the example.
You want a queue warning event sent once each minute.	queueMessageInterval	queueMessageInterval="60000"

The following examples show all of the queue parameters that are specified for the goals listed above:

```
<destination name = "incident_sender_slow" class =
"com.tivoli.RiskManager.Agent.Transports.Senders.rmaEIFSender" queueMaxSize =
"100000" queueThresholdSize="10000" queueMessageInterval="60000">
 </destination>

<destination name = "error_route" class =
"com.tivoli.RiskManager.Agent.Transports.Senders.rmaEIFSender" errorRoute="yes">
    <set key="RMA_conf" value="c:\IBM\RISKMGR\etc\error_route.conf"/>
</destination>
```

Examples of queue management events

This section provides examples of queue management events. Note that only partial events are shown.

- The following event informs you that the number of events that are queued has reached or exceeded the configured queue threshold size that is specified by the **queueThresholdSize** parameter.

  RMAgent_QueueProblem
  msg='QueueProblem:Component=db_sender:Reason=The queue threshold size has been exceeded.:currentSize=1001:thresholdSize=1000:maxSize=10000"
  severity=WARNING

- The following event informs you that the number of events that are queued is close to or has exceeded the configured queue maximum size that is specified by the **queueMaxSize** parameter.

  RMAgent_QueueProblem
  msg='QueueProblem:Component=db_sender:Reason=The queue maximum size has been exceeded.:currentSize=9992:thresholdSize=1000:maxSize=10000"
  severity=CRITICAL

- The following event informs you that the hard drive that the persistent queue is using has no more available space.

  RMAgent_QueueProblem
  msg='QueueProblem:Component=db_sender:Reason=The disk the queue is using has no more space available.:currentSize=999:thresholdSize=1000:maxSize=10000"
  severity=CRITICAL

- The following event informs you that the queue has failed and manual intervention is required.

  RMAgent_QueueProblem
  msg='QueueProblem Component=db_sender:Reason=The queue failed for an unknown reason.:currentSize=4567:thresholdSize=1000:maxSize=10000"
  severity=FATAL

wrmqueue -l command description

The description of the **-l** option of the **wrmqueue** command should be changed in the *IBM Tivoli Risk Manager Command Reference* as follows:

l or -list

This option lists information about the queues. The output is displayed in three sections and provides the following information in the order listed:

1. The queue name, status, and definition
2. The number of events in the queue
3. The number of failed events

The following output is an example of the **wrmqueue -l** output:

queue name	status	type	persist
summarization	Running	engine	yes
eif_sender1	Waiting(MAX)	sender	yes
eif_sender2	Running(THRESHOLD)	sender	no
eif_sender3	Waiting(DISKFULL)	sender	yes
eif_sender4	Failed	sender	no

queue name	# queued	# processed	#/second
summarization	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender1	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx

eif_sender2	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender3	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender4	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx

queue name	# failed
summarization	ttttttttt(rrrrrrrrr)
eif_sender1	ttttttttt(rrrrrrrrr)
eif_sender2	ttttttttt(rrrrrrrrr)
eif_sender3	ttttttttt(rrrrrrrrr)
eif_sender4	ttttttttt(rrrrrrrrr)

The following information describes the output that is provided by the **-l** option of the **wrmqueue** command:

Column heading	Description of information
queue name	The name of the queue.
status	The status of the queue (not the component). Status is indicated by one of the following values: Running — The queue is functioning without problems. Waiting(MAX) — The maximum queue size that was configured has been reached, and any components that are sending events to this queue are put in a wait state. Running(THRESHOLD) — The threshold queue size that was configured has been exceeded. Waiting(DISKFULL) — The disk that Tivoli Risk Manager persistent files are stored on is full and the agent is waiting until space is available. Failed — The queue has failed. Refer to the *Tivoli Risk Manager Problem Determination Guide* for information about resolving this problem.
type	The component type that is reading events from this queue: • engine • sender
persist	Indicates whether events are stored in memory or stored on a hard disk.
# queued	The number of events that are available for the component to process.
# processed	The number of events that were successfully processed since the agent was last started.
#/second	The number of events processed per second since either the last **wrmqueue -l** command was issued, or after the agent was restarted if this is the first time the **wrmqueue -l** command was issued.
# failed	*ttttttttt* is the total number of events that the component has not been able to process since the agent was last started. *rrrrrrrrr* is the number of failed queue attempts that will be retried when the agent is restarted.

5.3 Message and trace logging

This section provides information about the new first failure data capture (FFDC) function and other changes to Chapter 2 of the *IBM Tivoli Risk Manager Problem Determination Guide*, Message and Trace Logging and Other Diagnostic Tools.

Trace logging

The Tivoli Risk Manager product provides 3 levels of trace detail. The lowest level of detail, DEBUG_MIN, is the default level. At this level, only error conditions are traced. The next two levels are DEBUG_MID and DEBUG_MAX, which provide a greater detail of information. Levels can be modified by changing parameters in the logging configuration file or by calling the logging command line interface. Trace log data is currently only available in the English language.

A memory buffer is used by default to store all trace information. This minimizes the effect of tracing on system performance. The buffer is flushed to disk only when an exception occurs. You can also configure trace logging to write directly to disk, so that you can store trace data when no exception occurs. For examples of how to configure trace logging, see the "Tivoli Risk Manager Agent and Event Monitor Trace Customization" section.

The trace logs are located in the following files and directories:

- Tivoli Risk Manager C program trace logs on Linux and UNIX systems are located in /usr/ibm/tivoli/common/HRM/logs/<*application*>.error.log. The variable <*application*> specifies the name of the application.
- Tivoli Risk Manager C program trace logs on Windows systems are located in C:\Program Files\ibm\tivoli\common\HRM\logs\<*application*>.error.log. The variable <*application*> specifies the name of the application.
- Tivoli Risk Manager agent component trace logs for Linux and UNIX systems are located in /usr/ibm/tivoli/common/HRM/logs/traceHRM*n*.log.
- Tivoli Risk Manager agent component trace logs for Windows systems are located in C:\Program Files\ibm\tivoli\common\HRM\logs\traceHRM*n*.log.
- The Tivoli Risk Manager database utilities, wrmdbclose and wrmdbclear, write their trace records to separate files: traceHRM_DBClose.log and traceHRM_DBClear.log, respectively.

The Tivoli Risk Manager agent and event monitor trace records are written to sequentially numbered files named traceHRM*n*.log, where *n* is a number. The trace logger writes up to 5 files, each 1 MB in size. If more trace records are written than can fit in 5 MB, the trace files wrap. These trace file limits are all customizable using the logger configuration file. To change the number of trace files, use the **file.trace.maxFiles** parameter. To change the maximum size of each trace file, use the **file.trace.maxFileSize** parameter.

Most log messages are written to both the message log and the trace log. To ensure that all messages are written to the trace log, add the trace file to the listenerNames for the message logger as follows:

```
rmLogger.msg.listenerNames=file.message file.trace
```

First Failure Data Capture

First failure data capture (FFDC) is the snapshot of trace information at the time of an error condition. By customizing the trace logging configuration, you can cause a trace snapshot to be taken of either all errors or selected errors. Each snapshot creates a unique trace file which is not overwritten by subsequent trace snapshots. By default, FFDC is not active in the Tivoli Risk Manager product. It can be activated by changing the trace logging configuration. For information about changing the configuration, see section "Tivoli Risk Manager Agent and Event Monitor Trace Customization". FFDC snapshots are available only for the Tivoli Risk Manager agent and event monitor.

FFDC logs are located in the following files and directories:

On UNIX systems: /usr/ibm/tivoli/common/HRM/FFDC/*YYYY.MM.DD*/traceHRM*n*.log

On Windows systems: C:\Program Files\ibm\tivoli\common\HRM\FFDC*YYYY.MM.DD*\traceHRM*n*.log

The variable *YYYY.MM.DD* is the date on which the snapshot occurred and *n* is a number indicating the sequence of the snapshot on the given date.

Log XML

The following columns of the message and trace log records are used by the Tivoli Risk Manager product:

Time	Millis	Server
ServerFormat	ProductID	Component
LogText	SourceFile	SourceMethod
Thread	Exception	MessageId
TraceLevel	Severity	

Examples

The following query displays the contents of the message log file in ASCII:

```
viewer.sh -sascii /usr/ibm/tivoli/common/HRM/logs/msgHRM.log
```

The following query writes the contents of the trace log files in HTML to an external file:

```
viewer.sh  /usr/ibm/tivoli/common/HRM/logs/traceHRM*.log > trace_logs.html
```

The following query writes selected columns of the trace log files in HTML format to an external file:

```
viewer.sh -q "select
Time,Component,Thread,SourceFile,SourceMethod,LogText,EXCEPTION where true"
/usr/ibm/tivoli/common/HRM/logs/traceHRM*.log > trace_logs.html
```

The following query writes selected columns of ERROR messages from the message log file in HTML format to an external file:

```
viewer.sh -q "select
Time,MessageId,LogText,Component,Thread,SourceFile,SourceMethod where Severity
= 'ERROR'"  /usr/ibm/tivoli/common/HRM/logs/msgHRM.log > error_log.html
```

Tivoli Risk Manager Agent and Event Monitor Trace Customization

The Tivoli Risk Manager agent trace logging is controlled by the parameters in the $RMADHOME/etc/RMLogger.properties trace logging configuration file. For example, the **rmLogger.trc.level** parameter controls the amount of trace information that is gathered while the agent is running. The **rmLogger.trc.listenerNames** parameter controls whether trace information is written to memory or to a file on disk. To increase the amount of trace logging the agent performs, usually both of these parameters must be changed so that more information is captured and is written to the disk as it is created.

There are two ways to make changes to the trace configuration:

- Permanently by changing parameter values in the RMLogger.properties file and then restarting the agent

  For example, use the following procedure to permanently increase agent trace logging:

  1. Edit the $RMADHOME/etc/RMLogger.properties file to change the following parameters:
     ```
     rmLogger.trc.level=DEBUG_MAX
     rmLogger.trc.listenerNames=file.trace
     ```
  2. Restart the agent.

- Temporarily by changing parameter values using the logging command line interface (see section "Logging Command Line Interface"). Changes made by this method require that the agent is running and are in effect only while the agent is running.

  For example, use the following procedure to temporarily increase agent trace logging while the agent is running:

  1. Change to the $RMADHOME/logviewer directory.
  2. Enter the following commands from this directory:
     ```
     logcmd set rmLogger.trc level=DEBUG_MAX
     ```

```
logcmd set rmLogger.trc listenerNames=file.trace
```

The trace logs become larger as more information is logged. After the maximum number of trace files is reached, older trace data is overwritten by new data. The default trace configuration is 5 trace files at 1 MB each. To increase the trace file capacity to 10 files at 2 MB each, issue the following commands:

```
logcmd set file.trace maxFiles=10
logcmd set file.trace maxFileSize=2048
```

These settings only stay in affect as long as the agent is running; stopping and restarting the agent will cause these settings to go back to their default settings. To decrease agent trace logging while the agent is running, issue the following commands:

```
logcmd set rmLogger.trc level=DEBUG_MIN
logcmd set rmLogger.trc listenerNames=memory
```

To enable first failure data capture (FFDC) snapshots, customize the trace configuration as follows:

```
rmLogger.trc.listenerNames=snap.memory
rmLogger.msg.listenerNames=file.message ffdc.snap
```

All of these configuration changes affect all components of the Tivoli Risk Manager agent, including the event monitor. If you want to configure the event monitor differently from the rest of the agent, use rmLogger.trc.monitor in place of rmLogger.trc in the configuration file or in the command line interface. For example, to set event monitor trace logging to medium level and write to its own file, set the following parameters:

```
rmLogger.trc.monitor.level=DEBUG_MID
rmLogger.trc.monitor.listenerNames=file.trace.monitor
file.trace.monitor.fileName=trace_monitor.log
```

Issue the following command to list all defined trace loggers in the configuration:

```
logcmd list rmLogger.trc
```

Issue the following command to list the current settings for the trace logger:

```
logcmd config rmLogger.trc
```

Issue the following command to list the current settings for the event monitor trace logger:

```
logcmd config rmLogger.trc.monitor
```

5.4 Regular expression support

This section provides information about enhancements that were made to regular expression support for APAR IY53527. The following information about using regular expressions should be added to the *IBM Tivoli Risk Manager Administrator's Guide*:

Regular Expression Support

In IBM Tivoli Risk Manager, Version 4.2, the following new features are added to the event monitor that relies on the introduction of regular expression support to the Tivoli Risk Manager product.

- Prefilters
- Indexes
- Enhanced ability to specify event patterns

This new feature improves the overall performance, and simplifies the creation of format files. You can now express event patterns in the format files as regular expressions in addition to the simple wildcard tokens that were provided in prior releases.

To implement these new features, the regular expression library from Xerces is used. The Xerces regular expression matching engine is an implementation of a traditional (non-POSIX) Non-deterministic Finite Automaton (NFA) regular expression engine. The library supports most of the supported regular expression constructs as follows:

Construct	Symbol	Description	Example	Results
Simple Character Classes	[ ]	The basic form of a character class (or character set). Use this construct to match only one out of several characters.	gr[ae]y	Matches either gray or grey.
Negated Character Classes	[^]	Match all characters except those listed. Typing a caret after the opening square bracket negates the character class.	gr[^ae]y	Matches neither gray nor grey.
Repeating Characters	? * +	Match the preceding token zero or one time. Match the preceding token zero or more times. Match the preceding token one or more times.		
Shorthand Characters	\d \D \s \S \w \W	Match any digit Match any non-digit Match any white space character Match any non-white space character Match any word character: Match any non-word character:		
Dot	[.]	Matches almost any character. Use caution when using this construct. The dot (or period) is one of the most commonly used metacharacters and it is also the most commonly misused metacharacter.		
Anchors	 ^ $	Used to indicate a position, not match a character. They match a position before, after, or between characters and are used to anchor the regex match at a certain position. Indicates the start of a line. Indicates the end of a line.		
Word Boundries	 \b \B \w \W	Indicates word boundaries. Used to match whole words. The negated version of \b. Used to match non-word characters. The negated version of '\w'.	\b(is|art)\b	Matches either the word is or the word art.
Ranges	[-]	Used to specify a range of values. Note that you specify multiple ranges inside a character class or even combine ranges and single characters.	[0-9] [0-9a-fxA-FX]	Matches a single digit between 0 and 9. Matches a hexadecimal digit or the letter X.
Quantifiers	{}	Use quantifiers to further quantify expressions The ?, *, and + are also quantifiers.	{n} {n,} {n,m}	Match exactly *n* times. Match at least *n* times. Match at least *n* times, but not more than *m* times
Lookahead	(?=) (?!)	Matches the next character.	q(?=u) q(?!u)	Match a q followed by a u. Match a q not followed by a u.
Lookbehind	(?<=)	Matches the preceding character	(?<=a)b	Matches a letter b

			(?<!a)b	that is preceded by the letter a. Matches a letter b that is not preceded by the letter a.
Grouped Alternation	(a|e) gr[ae]y	Matches a single regular expression given several possible expressions. Note that if a '(' and ')' is specified at the beginning or end of an expression, the matching is not correctly implemented. This is caused by a problem with the Xerces library.	gr(a|e)y gr[ae]y (gray|grey)	Matches either gray or grey.

The following table lists the constructs that are not supported and an alternative construct that can be used.

Construct	Description	Alternative construct
Unions	Specifies a single character class that consists of two or more separate character classes. An example of a Union might be [0-4[6-8]], which should match any number from 0-8 with the exception of 5.	Specify [0-46-8], which avoids the nested brackets and achieves the same result.
Intersections	Specifies a single character class that matches everything that is common. An example of an intersection is [0-4&&[4678]], which would match the number 4. Intersections are similar to Unions and are used in similar circumstances.	Use the same alternative construct that is specified for unions.
Subtraction	Specifies a single character class that matches everything except what is common. Subtraction is essentially a negated intersection. An example of subtraction is [0-9&&[^345]], which would match any number from 0-9 with the exception of 3,4, and 5.	Specify the expression in a positive form. For example, [0-26-9].

6 Files added or replaced

This section lists the new and changed files for this fix pack. RMADHOME refers to the Tivoli Risk Manager installation directory, referenced by the RMADHOME environment variable.

/etc/init.d/rc.rmagent (Solaris and Linux)
/etc/rc.rmagent (AIX)
/etc/Tivoli/rma_eif_env.sh (remove LD_ASSUME_KERNEL on SUSE Linux version 8 and higher)
RMADHOME /bin/rma_webids-init (UNIX or Linux only)
RMADHOME/bin/RMCAH040201.sys (HPUX only)
RMADHOME/bin/RMCAL040201.sys (Linux only)
RMADHOME/bin/RMCAS040201.sys (Solaris only)
RMADHOME/bin/RMCAW040201.sys (Windows only)
RMADHOME/bin/RMCAX040201.sys (AIX only)
RMADHOME/bin/rmEventLog.dll (Windows only)
RMADHOME/bin/webids[.bat]
RMADHOME/bin/wrmadmin[.exe]
RMADHOME/bin/wrmdns (all except Windows & Solaris)
RMADHOME/bin/wrmqueue (all except Windows & Solaris)
RMADHOME/dbschema/rm_t_arc41_uc.ms.sql
RMADHOME/etc/incident_engine.conf
RMADHOME/etc/rmagent.dtd
RMADHOME/etc/rmclasspath.conf
RMADHOME/etc/RMLogger.properties
RMADHOME/etc/summary_engine.conf
RMADHOME/etc/tec/rules/riskmanager.wic
RMADHOME/etc/templates/baroc/rmagent.baroc
RMADHOME/etc/templates/incident_engine.conf
RMADHOME/etc/templates/rmagent.dtd
RMADHOME/etc/templates/rmclasspath.conf
RMADHOME/etc/templates/RMLogger.properties
RMADHOME/etc/templates/summary_engine.conf
RMADHOME/etc/templates/tec/rules/riskmgr_config.pro
RMADHOME/etc/templates/tec/rules/riskmanager.wic
RMADHOME/etc/templates/tec/rules/riskmgr_config.pro
RMADHOME/etc/tec/rules/riskmanager.wic
RMADHOME/lib/eif.jar
RMADHOME/lib/evd.jar
RMADHOME/lib/jffdc.jar
RMADHOME/lib/jlog.jar
RMADHOME/lib/rm_dbaccess.jar
RMADHOME/lib/rm_dbutil.jar
RMADHOME/lib/rm_util.jar
RMADHOME/lib/rmagent_msg.properties
RMADHOME/lib/rmagent.jar
RMADHOME/lib/rmeventmonitor.jar
RMADHOME/lib/rmsvrcfg.jar
RMADHOME/logviewer/logcmd.sh (UNIX or Linux only)
RMADHOME/logviewer/logcmd.bat (Windows only)
RMADHOME/msg_cat/C/rmeif.cat
RMADHOME/nids/templates/rules/www.rules
RMADHOME/reports/rm_ra_03.rpt (Windows only)
\Program Files/ibm/tivoli/common/HRM/scripts/getpd.bat (Windows only)
\Program Files/ibm/tivoli/common/HRM/scripts/getpdinfo.bat (Windows only)
/sbin/init.d/rc.rmagent (HP)
/usr/ibm/tivoli/common/HRM/scripts/getpdinfo (UNIX or Linux only)

7 Contacting software support

If you have a problem with any Tivoli product, refer to the following IBM Software Support Web site: http://www.ibm.com/software/sysmgmt/products/support/

If you want to contact software support, see the IBM Software Support Guide at the following Web site:

http://techsupport.services.ibm.com/guides/handbook.html

The guide provides information about how to contact IBM Software Support, depending on the severity of your problem, and the following information:

- Registration and eligibility
- Telephone numbers and e-mail addresses, depending on the country in which you are located
- Information you must have before contacting IBM Software Support

8 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 grant 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 Web sites. 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 which 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 measurement 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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM, the IBM logo, Tivoli, the Tivoli logo, AIX, DB2, Tivoli Enterprise Console, TME, pSeries, and zSeries are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are registered 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.

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

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

o

Printed in U.S.A.