



# **IBM Tivoli Risk Manager**

版本 **4.2** 修订包 **1**

自述文件

注：

在使用本资料及其支持的产品之前，请阅读第 34 页上的声明中的信息。

第一版（2004 年 9 月）

该版本适用于 IBM Tivoli Risk Manager V4.2 修订包 1 和所有后续发行版和修订版，直到在新版本中另有声明为止。

**Copyright International Business Machines Corporation 2004. All rights reserved.**

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP  
Schedule Contract with IBM Corp.

# 目录

<b>1 关于该修订包</b> .....	<b>4</b>
1.1 修订包内容.....	4
1.2 该修订包取代的补丁 .....	4
1.3 支持的操作系统 .....	4
1.4 该修订包中的新增内容.....	5
<b>2 安装和配置</b> .....	<b>6</b>
2.1 先决条件 .....	6
2.2 安装注意事项 .....	6
2.3 安装说明 .....	8
2.3.1 补丁安装.....	8
2.4 本地化包信息 .....	9
2.4.1 本地化包注意事项 .....	9
2.4.2 本地化包安装说明 .....	9
2.4.2.1 完全安装 .....	9
2.4.2.2 补丁安装 .....	9
<b>3 该修订包修正的 APAR</b> .....	<b>10</b>
<b>4 已知的局限</b> .....	<b>13</b>
4.1 安装 .....	13
4.2 关联服务器.....	13
4.3 Tivoli Enterprise Console 事件服务器 .....	13
4.4 Tivoli Risk Manager 代理程序 .....	14
4.5 DNS 解析 .....	15
4.6 消息和跟踪日志 .....	15
4.7 网络 IDS 组件 .....	16
4.8 Web IDS 组件 .....	16
4.9 Web 应用程序.....	16
<b>5 文档更新</b> .....	<b>18</b>
5.1 杂项文档修正 .....	18
5.1.1 IBM Tivoli Risk Manager 管理员指南 .....	18
5.1.2 IBM Tivoli Risk Manager 命令参考大全 .....	20
5.1.3 IBM Tivoli Risk Manager 安装指南 .....	20
5.1.4 IBM Tivoli Risk Manager 问题确定指南 .....	20
5.2 队列管理和操作 .....	21
5.3 消息和跟踪日志 .....	25
5.4 正则表达式支持 .....	28
<b>6 添加或替换的文件</b> .....	<b>31</b>
<b>7 联系软件支持</b> .....	<b>32</b>

8 声明 .....	34
------------	----

# 1 关于该修订包

本节提供有关该修订包的一般信息。请在安装该修订包前阅读该文档的全部内容。

本自述文档仅以 **Adobe Acrobat** 格式提供。

有关与该修订包一起提供的本地化包的信息，请参阅本自述文件中『**本地化包信息**』一节。

## 1.1 修订包内容

该修订包提供以下内容：

- 本自述文件
- 该修订包的映像报告
- 该修订包的 CD-ROM 映像

## 1.2 该修订包取代的补丁

该修订包取代了以下补丁：

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

## 1.3 支持的操作系统

本节列出该修订包支持的平台和数据库。

支持的操作系统版本 <sup>1</sup>	角色				可选组件			
	事件服务器	分布式关联服务器	网关	客户机	Crystal Reports	网络 IDS	Web IDS	Web 应用程序
AIX 5L V5.1 (32 位或 64 位)	X	X	X	X		X <sup>3</sup>	X	X
AIX 5L V5.2 (32 位或 64 位)	X	X	X	X		X <sup>3</sup>	X	X
Solaris 8 (SPARC) <sup>2</sup>	X	X	X	X		X	X	X
Solaris 9 (SPARC)	X	X	X	X		X	X	X
HP-UX 11i (32 位或 64 位)	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

支持的操作系统版本 <sup>1</sup>	角色				可选组件			
	事件服务器	分布式关联服务器	网关	客户机	Crystal Reports	网络 IDS	Web IDS	Web 应用程序
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

操作系统注意事项：

1. 该表中的信息基于提供该修订包时可用的信息。该表列举了由操作系统供应商指出的、使用期尚未结束的那些操作系统。有关当前支持信息，请参考 IBM 的联机支持。
2. Solaris 是指 Solaris Operating Environment，以下称为 Solaris。
3. 网络侵入检测系统（网络 IDS）在 64 位系统上不受支持。

RDBMS 供应商	版本
IBM DB2®	7.2 (FP8)、8.1 (FP2)
Oracle	9i、9i v2
Sybase	12
Microsoft SQL Server	7.0、2000

## 1.4 该修订包中的新增内容

本节提供有关已对 Tivoli Risk Manager 产品作出的更改的信息。

- 对管理队列的支持得到了加强。现在提供了关键字，从而提供了一种控制队列大小和发送有关队列状态的事件的方法。有关更多信息，请参阅『文档更新』一节。
- 对正则表达式的支持得到了加强。现在使用一种更健壮、最新版本的 Xerces 正则表达式库，提供了对标准正则表达式语法的更广泛的支持。有关更多信息，请参阅『文档更新』一节。
- 增加了对首次失败数据捕获的支持。有关更多信息，请参阅『文档更新』一节。
- RMAgent\_Inactive 事件中包含的 msg 属性已得到了加强，包括了不再发送 RMAgent\_HeartBeat 事件的代理程序的主机名和 IP 地址。有关更多信息，请参阅『文档更新』一节。
- 现在提供了对 Windows 2003 Server 的支持。

## 2 安装和配置

### 2.1 先决条件

以下软件是 Tivoli Risk Manager 修订包 1 所必需的：

- IBM Tivoli Risk Manager V4.2
- 带 FP01 的 IBM Tivoli Enterprise Console V3.9（仅针对事件服务器角色。）
- 对于 Red Hat Enterprise Linux，建议的 Java 运行时版本为 IBM JRE 1.3.1-6 或更高版本。如果您无法使用这些版本，请联系 IBM 软件支持。

### 2.2 安装注意事项

本节提供有关安装 Tivoli Risk Manager 产品的附加信息。

- 如果您安装了 Tivoli Risk Manager 4.2.0-RMG-FP01 修订包并要安装 Tivoli Risk Manager 产品的初始安装过程中未安装的可选组件（例如，Crystal Reports），请联系 IBM 软件支持以获取执行该过程所必需的安装修订包。
- 可以将该修订包以完全安装来安装或安装为补丁。有关确定应该使用的方法的更多信息，请参阅『安装说明』一节。
- Windows 事件监视器创建注册表键以标出上一次读取 Windows 事件日志的位置。这些项用于确定重新启动事件监视器或 Tivoli Risk Manager 代理程序时开始读取事件的位置。卸载 Tivoli Risk Manager 产品时，卸载程序不会从注册表除去这些注册表键。如果您重新安装事件监视器，则会在下次启动事件监视器时使用原有的注册表键，且事件监视器会开始读取原有事件。为了确保 Windows 事件监视器仅从当前日期开始读取事件且不会读取原有事件，请在第一次启动事件监视器之前删除以下事件监视器注册表键：  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Tivoli\Riskmgr\Agent\RMLogfile
- 在 Solaris 系统上安装 Tivoli Risk Manager Web 应用程序组件的过程可能非常缓慢或者可能会停止。可能将缺省的最大打开文件数设置得过低，以至于 WebSphere Application Server 无法成功安装 Tivoli Web 应用程序组件。这会导致 WebSphere Application Server 连续重试安装过程而不是返回错误代码。

可通过发出以下命令来确定文件描述符限制：

```
ulimit -n
```

要在 WebSphere Application Server 上成功安装 Tivoli Risk Manager Web 应用程序组件，必须在使用以下某个过程安装 Tivoli Risk Manager Web 应用程序之前用不小于 1024 字节的最大文件描述符开始安装（假定使用 Tivoli Enterprise Console Web 应用程序安装样本 WebSphere Application Server 应用程序）。但是在执行该操作之前，应该先阅读 Solaris 文档以了解进行这些更改的预防措施、执行过程和结果。根据安装的 WebSphere Application Server 应用程序的数量，可能需要更改最大文件描述符的精确值。

使用以下某个方法来更改最大文件描述符：

1. 停止 WebSphere Application Server。
2. 发出以下命令：  
ulimit -n 1024
3. 从发出 ulimit 命令的同一个命令会话重新启动 WebSphere Application Server。
4. 安装 Tivoli Risk Manager 产品。

一个更为长久的解决方案是通过在 `/etc/system` 文件中设置以下属性来更改文件描述符的系统值：

```
rlim_fd_cur
rlim_fd_max
```

- 对于带 Sybase 数据库的 Tivoli Risk Manager 产品的新安装，在 Tivoli Enterprise Console 产品数据库的缺省段中安装了 Tivoli Risk Manager 表。Tivoli Enterprise Console 安装定义的缺省段非常小，它仅保留了数量非常有限的 Tivoli Risk Manager 归档表事件。要使用带 Sybase 上的缺省实现的 Tivoli Risk Manager 产品，可以通过再添加一个设备来增加 Tivoli Enterprise Console 数据库中的缺省段。以下过程提供一个示例，指示如何通过名为 `TEC_SYSTEM_2` 的缺省段中创建一个 200 MB 设备来增加缺省段大小。

注：

- ALTER DATABASE 语句会自动将新设备添加到缺省段。
- 使用 Sybase 系统的用户标识设置 Sybase 环境，以便执行该过程。该用户标识必须具有适当的权限和 Sybase 环境。

- 如下所示，创建名为 `rm_exp_archive_table.syb.sql` 的脚本文件：

```
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
```

- 评估以下参数并对它们进行更改以满足您的安装要求：

- DISK INIT name:** 选择您的安装相应的名称。
- physname:** 指定所要创建的设备的操作系统路径名。
- vdevno:** 确保这是一个未使用的数字。使用以下命令来确定当前使用的数字：`select distinct low/16777216 from sysdevices`

- 发出以下命令来运行脚本：

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

变量 `<pw>` 是 SQL 密码，变量 `<system>` 是安装数据库的系统名。

- 安装过程中显示以下消息则表示无法找到 Java 可执行文件：

"未找到 JVM"

这可能是由包含临时目录的文件系统上没有足够的可用空间所导致。如果这是导致问题的原因，则可以执行以下操作之一：

- 释放该文件系统中的空间
- 向该文件系统分配更多空间

所需空间最多可达已安装的 Java JRE 大小的三倍。

- 如果您重新安装 Tivoli Risk Manager 产品并将传送类型更改为 TME，则请在 `/etc/Tivoli/rma_eif_env.sh` 脚本文件中将 **TMEEndpoint** 关键字的值更改为 `true`，如下所示：

```
TMEEndpoint=true
```



## 2.3 安装说明

本节提供有关安装该修订包的信息。

可以按照完全安装或补丁安装方式来安装 Tivoli Risk Manager 4.2.0-RMG-FP01 修订包。完全安装必须在以下条件下执行：

- 您要将 Web 应用程序与除 DB2 外的任何 RDBMS 产品一起使用。
- 您要将该修订包安装到以下某个平台上：

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)

请联系 IBM 软件支持以获取进行完全安装时必须使用的安装包。

### 2.3.1 补丁安装

请发出以下命令来安装补丁：

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

请为 <platform> 指定以下某个平台：

AIX: Tivoli Risk Manager 产品支持的 AIX 版本  
HP-UX: Tivoli Risk Manager 产品支持的 HP-UX 版本  
Linux: Tivoli Risk Manager 产品支持的 Linux (IA32) 版本  
LinuxPPC: Tivoli Risk Manager 产品支持的 Linux (PPC) 版本  
Solaris: Tivoli Risk Manager 产品支持的 Solaris (SPARC) 版本  
Win: Tivoli Risk Manager 产品支持的 Windows 版本

您可以指定以下某个选项：

-silent 该选项无需用户输入。请检查安装目录中的日志文件以查找非零返回码，以便确定安装是否成功。  
-console 该选项提供终端（文本模式）安装。请注意，该选项在 Windows 平台上不可用。

如果您未指定选项，则会显示以下窗口：

- 语言
- 欢迎页面
- 安装前
- 安装后

用户无需在这些窗口输入任何内容。每个窗口显示时，请单击下一步。

如果您在事件服务器上安装了该修订包，则请在完成安装之后执行以下过程：

1. 请确保您要使用的规则库是当前的规则库。
2. 发出以下命令：  
**rmcorr\_cfg -update**

注：该命令会更新规则库。它还会停止并重新启动 Tivoli Enterprise Console 事件服务器。

## 2.4 本地化包信息

4.2-RMG-FP01 修订包所包含的本地化包包含 Tivoli Risk Manager V4.2 产品支持的所有语言的已更新翻译。本节提供以下本地化包信息：

- 本地化包注意事项
- 本地化包安装说明

### 2.4.1 本地化包注意事项

在安装 4.2-RMG-FP01 修订包之前，请查看本节中的信息。

- 该修订包中包含的已更新国际语言资源反映了 Tivoli Risk Manager 用户界面和消息的改变。
- 完全安装和补丁安装之前的差别在于安装的文件数量和安装前执行的必备软件检查。
- 补丁安装过程中显示的窗口与完全安装过程中显示的窗口相同。

### 2.4.2 本地化包安装说明

本节提供本地化包安装信息。可以按照完全安装或补丁安装方式来安装 Tivoli Risk Manager V4.2 修订包 01 的本地化包。如果您执行基本产品的完全安装，请使用完全安装（有关更多信息，请参考以上『安装说明』一节。）如果您执行基本产品的补丁安装，请使用补丁安装。

#### 2.4.2.1 完全安装

要执行国际语言资源的完全安装，请参阅《*IBM Tivoli Risk Manager 发行说明 V4.2*》的『国际语言支持』一节中的安装说明。

#### 2.4.2.2 补丁安装

要执行补丁安装，请发出以下某个命令：

对于 Windows 平台：

```
rm1p4201_setupwin32.exe
```

对于 UNIX 和 Linux 平台：

```
./rm1p4201_setup<platform>.bin
```

请为 <platform> 指定以下某个平台：

AIX:	Tivoli Risk Manager 产品支持的 AIX 版本
HP-UX:	Tivoli Risk Manager 产品支持的 HP-UX 版本
Linux:	Tivoli Risk Manager 产品支持的 Linux (IA32) 版本
LinuxPPC:	Tivoli Risk Manager 产品支持的 Linux (PPC) 版本
Solaris:	Tivoli Risk Manager 产品支持的 Solaris (SPARC) 版本

对于 Linux for zSeries (S/390)：

```
java -Dis.java.home=/opt/IBMJava2-s390-131/jre -cp ./rm1p4201_setup.jar run
```

### 3 该修订包修正的 APAR

本节提供 4.2.0-RMG-FP01 修订包提供的 APAR 修正包的描述和解决方案。

#### APAR: IY48016

症状：同一个系统上运行多个 Web 侵入检测系统（Web IDS）实例时，由于所有广泛实例使用同一份 `webids.lastread` 文件，所以恢复功能不正常。

解决方案：现在每个 Web IDS 功能实例均使用其自身的 `webids.lastread` 文件。

#### APAR: IY50483

症状：在 Tivoli Risk Manager 或 Tivoli Enterprise Console 服务器上，`tec_rule` 进程表现出 CPU 使用率过高。这会导致入局事件保持在 `QUEUED` 状态。

解决方案：已对生成事件组的 Tivoli Risk Manager Tivoli Enterprise Console 规则进行了修改以提高性能。已向 `$RMADHOME/etc/tec/rules` 目录中的 `riskmgr_config.pro` 文件添加了用于事件组处理的其它配置选项。有关使用这些选项的更多信息，请参阅 `riskmgr_config.pro` 文件中的注释。

#### APAR: IY52322

症状：接收到部分事件时分布式关联服务器停止。

解决方案：使用新的 Tivoli Enterprise Console API 关键字 **ReadRetryInterval** 来配置在接收到部分事件时 Event Integration Facility API 使用的超时值。

该关键字的缺省值是 120 秒。

Event Integration Facility 发送器处理大于 2 KB 的事件时，会将事件分为两个使用套接字连接传递的数据包。如果接收器确定该事件为部分事件，则它将在检索第二个数据包和完成该过程之前等待由该关键字指定的时间段。如果在该时间段中没有接收到第二个数据包，则将废弃收到的部分事件并将消息写入日志。

#### APAR: IY52323

症状：重新启动系统时未关闭 Tivoli Risk Manager 代理程序之间的未使用套接字连接。

解决方案：现在会自动关闭代理程序间未使用的套接字连接。

#### APAR IY53525

症状：在 UNIX 系统上，事件监视器不读取转储日志文件时创建的新日志文件。

解决方案：现在事件监视器可正确读取新日志文件。

#### APAR IY53527

症状：需要为事件监视器支持的正则表达式语法提供文档。

解决方案：改进了对正则表达式的支持并提供了文档。有关文档更改，请参阅『文档更新』一节。

#### APAR: IY53678

症状：事件监视器对与某个类的索引模式匹配的事件，而不是对 XML 文件中为该类定义的类模式进行语法分析时生成 Java 空指针异常。

解决方案：更改了事件监视器处理，这样如果事件字符串与某个类的索引模式（而非类模式）匹配时，不会认为它与该类匹配，而会继续搜索另一个匹配的类。

#### APAR: IY53713

症状：将一组事件插入数据库且该插入不完全成功时接收到重复的密钥异常。

解决方案：将事件插入数据库的操作现在正常完成。仅将每个事件插入一次。如果检测到重复的密钥，则会加强处理以废弃重复的事件。

#### APAR: IY54408

症状：因为系统内存不足，所以重复使用 **wrmadmin -i** 命令导致系统停止。

解决方案：现在可以反复使用 **wrmadmin -i** 命令而不再引起系统内存问题。

#### APAR: IY54568

症状：Windows 事件日志事件监视器重新处理已经处理过的事件。

解决方案：不再对事件进行反复重新处理。

#### APAR: IY55241

症状：应该更新网络 IDS 文件以使其包括 CAN-2002-0562 漏洞的正确签名。

解决方案：签名文件得到更新，包含了正确的签名。

#### APAR: IY55319

症状：队列中有大量事件时 **wrmqueue** 命令未完成。

解决方案：已对与 **wrmqueue** 命令相关的内部过程进行更改，以便改正该问题。有关该命令的更多信息，请参阅『文档更新』一节。

#### APAR IY55895

症状：《*IBM Tivoli Risk Manager 适配器指南*》和与各种适配器程序包一起提供的其它 PDF 文档引用事件映射表。Web 站点上未提供该表，因此无法进行下载或引用。

解决方案：现在 Risk Manager 支持 Web 站点

<http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliRiskManager.html> 上提供了事件映射表文档（DCF 1171204）。

#### APAR IY55927

症状：运行于 DBCS 语言环境中时，Tivoli Risk Manager 代理程序废弃包含 DBCS 字符的事件。会在 Tivoli Risk Manager 消息日志中写入以下消息：

HRMAG0135W 事件集成工具 TECAgent 过滤了以下事件

解决方案：Tivoli Risk Manager 代理程序现在正确处理包含 DBCS 字符的事件。

APAR: IY56431

症状：如果使用区分大小写的选项安装 Microsoft SQL，则 Tivoli Risk Manager 事件库不支持 Microsoft SQL。以下症状表示存在该问题：

- 未将事件写入 Microsoft SQL 事件归档。
- 会在 Tivoli Risk Manager 消息日志中写入以下错误消息：  
HRMAG0082E SQL exception:[Microsoft] [SQLServer 2000 Driver for JDBC]  
[SQLServer]Invalid object name 'RM\_T\_ARC41'

解决方案：发出以下命令来运行修正该问题的 DDL 文件：

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

## 4 已知的局限

本节提供对每个局限和变通方法（如果可用）的描述。

### 4.1 安装

局限：安装过程中会显示以下不正确警告消息：

警告：无法复制日志输出 /opt/RISKMGR/rminstall\_log.txt

（该文件或目录不存在）

变通方法：如果您怀疑安装过程中出现错误，则请重新安装 Tivoli Risk Manager 产品并在安装命令中指定以下选项以在除 /opt/RISKMGR 以外的目录中创建日志：

-l !<fully qualified path>

变量 <fully qualified path> 是 rminstall\_log.txt 文件的标准路径。

### 4.2 关联服务器

局限：未将 Tivoli Risk Manager 代理程序事件（例如 RM\_Sensor、RM\_Error、RMAgent\_Inactive 和 RMAgent\_QueueProblem）发送到 Tivoli Enterprise Console 产品，且不在事件控制台上显示这些事件。该问题仅适用于符合以下两个条件的系统：

- 您的安装是事件服务器安装或分布式关联服务器安装
- 您没有执行缺省安装。而是选择仅向 Tivoli Enterprise Console 服务器发送突发事件（RM\_Incident）。有关安装选项的更多信息，请参阅《Tivoli Risk Manager 安装指南 V4.2》第 102 和 114 页。

变通方法：要解决该问题，请使用以下过程

1. 编辑您的关联服务器和事件服务器上的 \$RMADHOME/etc/rmagent.xml 文件并添加以下过滤器定义：

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

2. 通过修改 <withfilter name ="incidents"/> 语句更改现有的连接符定义，以便指定新的过滤器名称 nonSensorEvents，如下所示：

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

3. 重新启动代理程序以使更改生效。

### 4.3 Tivoli Enterprise Console 事件服务器

局限：一旦将 RMAgent\_Inactive 和 RMAgent\_QueueProblem 事件发送到事件控制台，这些事件就会与其它传感器事件混合在一起，并在 RM\_SensorEvent 分组视图中显示。如果您为 Tivoli 事件控制台或分

布式关联服务器部署了缺省配置，则 **RM\_SensorEvent** 分组视图可能包含很多事件。这就使得识别警告您的网络中出现的 **Tivoli Risk Manager** 代理程序和队列问题的 **Tivoli Risk Manager** 代理程序事件的过程变得困难。

变通方法：要使得监视代理程序问题的过程变得更容易，请使用以下过程在事件控制台中定制 **RM\_Error** 分组视图，使其包含 **RMAgent\_Inactive** 和 **RMAgent\_QueueProblem** 事件：

1. 在事件控制台主视图中单击 **Windows** → 配置。
2. 在左侧窗格中单击事件组。
3. 单击 **RM\_Error**。
4. 右键单击该窗口并单击创建过滤器。显示“添加事件组过滤器”窗口。
5. 在名称字段中输入 **RM\_AgentProblem**。
6. 在描述字段中输入对该过滤器的可选描述。
7. 单击添加约束。
8. 从属性列表中选择类。
9. 从操作员列表中选择 **Like**。
10. 为该值输入 **RMAgent\_%**。（该值区分大小写。）
11. 单击确定。
12. 在“添加事件组过滤器”窗口中单击测试 **SQL** 以确定过滤器是否产生正确数量的事件。
13. 单击确定以保存更改。
14. 停止和重新启动事件控制台。
15. 单击 **Windows** → 总结图表视图并打开 **RM\_Error** 控制台组以确定过滤器是否正常运行。

## 4.4 Tivoli Risk Manager 代理程序

- 局限：内存约束可能导致内存不足问题。该问题在 **AIX** 系统上最为明显。在接收器或发送器的数量增加或将 **instanceCount** 参数添加到任何 **rmagent.xml** 目标定义时都可能出现该问题。在您添加大量发送器或大量 **instanceCounts** 时，也可能在其它平台上出现该问题，因为这两个选项都会产生附加线程并增加内存使用。

**Tivoli Risk Manager** 代理程序为 **Java** 进程，受 **Java** 环境的内存分配的约束。在 **AIX** 上，该内存限制受 **/etc/security/limits** 文件中存储量分配的低缺省值的显著影响。要使 **Tivoli Risk Manager** 在缺省 **AIX** 安装中运行，有意通过 **RmagentMemMax** 参数限制最大 **Java** 存储量，其中该参数在 **RMADHOME/etc/rmad.conf** 文件中进行了定义。在 **AIX** 上将该值设置为 **92 MB**，这仅提供了基本服务器安装所需的足够内存分配。

变通方法：可在任何平台上使用 **RmagentMemMax** 参数来增加 **Tivoli Risk Manager** 可用的最大内存。例如，在 **AIX** 上执行以下过程：

1. 增加界限文件中 **data**、**rss** 和 **stack** 值的缺省值（或使用 **ulimit** 命令）
  2. 增加 **rmad.conf** 文件中的 **RmagentMemMax** 值。
  3. 注销然后登录系统。
  4. 发出 **wrmadmin -r** 命令以重新启动 **Tivoli Risk Manager** 代理程序。
- 局限：如果持久性目录所处的磁盘已满，则无法重新启动 **Tivoli Risk Manager** 产品。

变通方法：在重新启动 Tivoli Risk Manager 产品之前确保有足够的可用磁盘空间。请使用以下公式来确定所需的磁盘空间数量：

$$(1 + \text{目标数}) \times 20 \text{ MB}$$

目标数是 `rmagent.xml` 文件中定义的目标的数量。

- 局限：如果某个事件属性的第一个字符为单引号，则该事件损坏，因为该单引号和该事件属性的最后一个字符被除去。以下示例显示为 `msg` 事件属性指定的前导引号和结果：

`'myHostname' is acting suspiciously`

归档表中相应的 `MSG` 列将包含以下内容：

`myHostname' is acting suspiciousl`

变通方法：如果可能，避免在事件属性中使用前导单引号。否则，没有可用的变通方法。

## 4.5 DNS 解析

局限：对于 Solaris，`wrmdns` 命令不会启动 DNS 解析。

变通方法：要启动 DNS 解析，请执行以下过程：

1. 编辑 `summary_engine.conf` 文件和 `incident_engine.conf` 文件。
2. 将这两个文件中的 `dnsResolver=off` 项更改为 `dnsResolver=on`。
3. 发出以下命令来重新启动 Tivoli Risk Manager 代理程序：

`wrmadmin -r`

## 4.6 消息和跟踪日志

- 局限：在某些 Linux 系统上，可能无法动态更改跟踪和日志级别设置，因为 Linux 的缺省 IP 过滤和防火墙保护限制性很强。

Tivoli Risk Manager 产品中包含的 JLog 程序包提供在 Tivoli Risk Manager 代理程序运行时动态更改跟踪和日志设置的能力。有关该功能的更多信息，请参阅《*IBM Tivoli Risk Manager 问题确定指南*》的『记录命令行界面』一节。

Tivoli Risk Manager 代理程序启动时会调用 JLog 日志管理器，该管理器会创建侦听端口 9992 的日志命令服务器。`logcmd` 客户机程序通过该端口与日志命令服务器通信。在某些 Linux 系统上，Tivoli Risk Manager 代理程序运行时端口 9992 未侦听且由于 `Java ConnectionException` 而导致 `logcmd` 命令失败。这是由安装的 IP 过滤器和防火墙保护导致的。如果以下某个程序安装在您的 Linux 系统上且 Tivoli Risk Manager 代理程序启动时无法观察到端口 9992 侦听，则是因为 IP 防火墙阻止访问该端口：

- `lokkit`
- `ipchains`
- `iptables`
- `ipfwadm`

变通方法：请参考您的 Linux 系统文档以了解对端口 9992 进行解锁的过程。如果出于安全考虑要使该端口处于锁定状态，则除无法动态更改跟踪设置的情况外，不会干扰标准 Tivoli Risk Manager 代理程序记录。

- 局限：在 UNIX 系统上，转储日志文件时会将其压缩，从而主机 IDS 适配器无法读取这些文件。

变通方法：为防止出现该问题，请关闭最近转储的日志文件的日志压缩功能。

- 局限：以下消息（`HRMAG0147I`）并不总是紧跟在重复的消息后面：



上一条消息已重复 {n} 次

在这种情况下无法确定重复了哪条消息。

变通方法：没有可用的变通方法。

## 4.7 网络 IDS 组件

局限：在 32 位 AIX 系统上启动网络 IDS 组件时，该组件可能不启动。这可能是因为未定义网络 IDS 组件用来监视网络的 /dev/bpf0 设备，或上次重新引导系统以来未正确启动该设备。

变通方法：使用以下过程重置或定义 /dev/bpf0 设备：

1. 从 AIX 终端会话发出 **tcpdump** 命令。
2. 在显示以下消息后按 **Ctrl+C** 来终止 **tcpdump** 命令，从而表示已启动了以太网连接：

侦听 xxx

字母 xxx 代表以太网设备号，例如 en0。

3. 请发出以下命令来停止和重新启动网络 IDS 进程：

stopnids

startnids

## 4.8 Web IDS 组件

- 局限：通过在 **webids.cfg** 文件中写入代码 **fileMatch\_value=0** 来禁用 Web IDS 组件的日志文件翻转会导致显示错误消息。  
变通方法：该问题没有变通方法。不能禁用日志文件翻转。
- 局限：如果将 Web IDS 组件配置为在同一个系统上监视多个 Web 服务器且这些服务器的访问日志都位于同一个目录中，则该 Web IDS 组件会循环。  
变通方法：将 Web 服务器访问日志存储在不同的目录中。
- 局限：**webids -d** 命令不将调试信息写到标准输出（STDOUT）。有关更多信息，请参阅『文档更新』一节。  
变通方法：没有可用的变通方法。

## 4.9 Web 应用程序

- 局限（APAR IY58098）：如果运行 Java 控制台的系统不在运行 WebSphere Application Server 的本地子网上，则可能无法登录 Tivoli Risk Manager Web 控制台。这是因为安装 Tivoli Risk Manager Web 应用程序时，使用短主机名而不是运行 Web Application Server 的系统的标准主机名来更新 **rmweb.pl** 脚本。  
变通方法：请执行以下过程来指定 Web Application Server 的标准主机名：
  1. 编辑位于事件服务器的 **RMADHOME/cgi-bin** 目录中的 **rmweb.pl** 脚本。
  2. 找到以下行（大约第 47 行）：  

```
$output .= "METHOD=POST ACTION=\"http://server1:9080/rmwebapp42/logon\">");\n";
```
  3. 将 URL 字符串中的短主机名更改为标准主机名（例如 **server1.mycompany.com.**）
- 局限：如果安装了过期的 Mozilla 版本，则可能无法使用 Web 应用程序。  
变通方法：安装 Mozilla V1.7.2 或更高版本。

- 局限：卸载 Tivoli Risk Manager Web 应用程序之后，Tivoli Risk Manager JDBC 提供程序仍然作为 WebSphere Application Server 资源存在。

变通方法：使用以下过程除去 Tivoli Risk Manager JDBC 提供程序：

1. 以管理员身份登录 WebSphere Application Server 管理员控制台。
  2. 单击资源。
  3. 单击 **JDBC**提供程序。
  4. 确保将范围设置为服务器级别。
  5. 选择 **Risk Manager JDBC** 提供程序复选框。
  6. 单击删除。
- 局限：联机帮助存在对适配器地址帮助的不正确引用。在“系统地址”窗口中单击问号（?）时，帮助面板显示以下选择以获取系统信息：

源地址  
目标地址  
传感器地址  
适配器地址  
其它

变通方法：没有变通方法。适配器地址的信息不可用。

## 5 文档更新

本节提供了对 Tivoli Risk Manager V4.2 库的文档更新的描述。阅读以下部分中的信息以了解应对库进行的修正并了解已对 Tivoli Risk Manager 产品作出的改进：

- 杂项文档更新
- 队列管理和操作
- FFDC 和其它跟踪文档
- 正则表达式支持

### 5.1 杂项文档修正

本节提供了有关应对 Tivoli Risk Manager 库进行的杂项文档修正以及已对该修订包作出的次要功能更改的文档的信息。

#### 5.1.1 IBM Tivoli Risk Manager 管理员指南

- 应将以下文本添加到第 101 页的『定制基于突发事件的相关规则』一节：

该规则的 `<threshold>` 和 `<aggregate>` 元素确定何时生成突发事件。Tivoli Risk Manager 产品随附的缺省规则通过累计每个传感器事件的 `rm_Level` 值直到 `thresholdCount` 值已达到（在此生成突发事件）来聚集事件。`rm_Level` 值代表每个事件的相对权重或严重性。备用方法是计数事件的数量，并当计数达到特定阈值计数时生成突发事件。要启用计数事件，从规则中删除 `<aggregate>` 元素并调整 `thresholdCount` 参数以表示生成突发事件所需的事件的数量。

规则的 `<cloneable>` 元素中的 `attributeSet` 参数确定来自事件的哪个属性用于将进入的事件聚集作为可能突发事件的候选。在该参数中使用的三个标准相关属性是 `rm_SourceToken`、`rm_DestinationToken` 和 `rm_CategoryToken` 属性的任何组合。以下是可在 `attributeSet` 参数中指定的可用属性名称的列表。除非另外注明，否则规则中使用的属性名称与来自进入事件的属性名称相同。

- `rm_SensorToken`
  - `rm_SourceToken`
  - `rm_DestinationToken`
  - `rm_CategoryToken`（`rm_ClassCategory` 的同义词）
  - `rm_CategoryDescription`（`rm_ClassCategoryDescription` 的同义词）
  - `rm_CustomerID`
  - `rm_Signature`
  - `rm_Timestamp32`
  - `rm_Level`
- 应对第 103 页中『将属性设置为特定值』一节进行以下更改：

规则的 `<action>` 元素中的 `<parameters>` 元素可用于更改任何 `RM_Incident` 事件属性的值（除了 `hostname` 和 `msg` 属性）。

第 103 页的第二个示例指定 `msg` 属性；该示例不正确，应删除。
- 第 125 页的『资源标识和动态数据』一节的第一段应该更改如下：

资源标识和动态数据：这些区域中显示的文本由硬编码的文本或者资源标识指定。

硬编码文本是编码文本的一种更为简便的方法，因为您只需更新一个文件且无须停止并重新启动 WebSphere 产品以使更改生效。请注意，如果您使用的是带有本地化包的 Tivoli Risk Manager 产品，则应使用资源标识方法。

要使用硬编码文本，请以 `&quot;` 开始和结束文本字符串。使用以下步骤以硬编码文本。

1. 编辑 `AdvisorRules.xml` 文件。
2. 将下行添加到该文件：  
`title="&quot;View CVE Recommendation &quot;."`
3. 保存 `AdvisorRules.xml` 文件。

当显示 Web 页面时，“查看 CVE 推荐”将在标题区中显示。

您还可以通过编码指定事件或突发事件属性的字符串中的变量来在硬编码文本内使用动态数据。例如，要在硬编码文本内显示 `rm_Category` 属性值，步骤 2 中的文本将编码如下：

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

第 125 页的『资源标识和动态数据』一节的其余部分未更改。查看这些信息以了解有关动态数据以及使用资源标识的更多信息。

- 第 47 页的『过滤属性』一节应该更改如下：

#### 过滤属性

您可以过滤属性，这样它们将不会发送至 Tivoli Enterprise Console 服务器。

您可以将配置选项添加到位于代理程序和分布式关联服务器的 `EIF_sender.conf` 文件，以便不将某些扩展槽发送至 Tivoli Enterprise Console 服务器。

例如，将下行添加到 `EIF_sender.conf`：

`filterAttributes=/opt/RISKMG/ETC/TEMPLATES/sensorevent_attributeFilter.xml`

有关该过滤的示例，请参阅 `RMADHOME /etc/templates/sensorevent_attributeFilter.xml` 文件。

- 以下关键字应该记录于附录 A『事件集成工具发送器和接收器关键字』中：

#### **filterAttributes=pathname ...**

指定包含属性过滤规范的一个或多个 XML 文件的全路径名。规范可用于在事件传送之前从该事件过滤出扩展属性。属性过滤对于正将事件发送至 Tivoli Event Console 服务器的事件集成工具发送器子组件很有用，可以排除不需要的网络流量并改进性能。

有关样本属性过滤规范文件，请参阅以下文件：

`RMADHOME /etc/templates/sensorevent_attributeFilter.xml`

#### **ReadRetryInterval=seconds**

指定当收到部分事件时事件集成工具接收器等待的秒数。如果接收器确定事件为部分事件，则在检索第二个数据包并完成该过程之前它将等待由该关键字指定的时间段。如果在该时间段中没有接收到第二个数据包，则将废弃收到的部分事件并将消息写入日志。缺省值为 120 秒。

- 第 192 页的『手动配置事件监视器』一节在步骤 3 中提供不正确的示例。具有 `<source name="monitor_receiver_webids"` 的行应如下更改为 `<source name="monitor_receiver_nids"`：

```
<!-- Event Monitor for NIDS -->
<source name="monitor_receiver_nids"
class="com.tivoli.RiskManager.Agent.Transports.Receivers.rmaMonitorReceiver">
```

```
<set key="RMA_conf" value="/opt/RISKMGREtc/monitor_receiver_nids.conf"/>
</source>
```

- 第 87 页的『脉动信号监视』一节应更改如下：

Tivoli Risk Manager 自动监视部署在网络中的代理程序，且当代理程序变得不活动时警告您。该警告是在您的关联服务器之一生成的 **RMAgent\_Inactive** 事件。RMAgent\_Inactive 事件包含在 Tivoli Enterprise Console 数据库中，并可在控制台上查看。显示以下警告消息：

缺少代理程序的脉动信号：<hostname>/<ip address>

<hostname> 和 <ip address> 是不再发送 RMAgent\_HeartBeat 事件的代理程序的主机名和 IP 地址值。

在缺省情况下，每个代理程序配置为生成 RMAgent\_HeartBeat 事件。当代理程序停止发送常规的 RMAgent\_HeartBeat 事件时，每个关联服务器都配置为监视 RMAgent\_HeartBeat 事件并生成 RMAgent\_Inactive 事件。在缺省情况下，将有一个已创建的 RM\_Sensor 事件表示生成 RMAgent\_HeartBeat 事件的每个代理程序。RMAgent\_HeartBeat 事件通常并不转发 Tivoli Enterprise Console 服务器或数据库。

### 5.1.2 IBM Tivoli Risk Manager 命令参考大全

第 25 页的“您可以使用 **webids -d** 命令来将调试信息写入标准输出（STDOUT），您可以随后将其重定向到另一个文件”的陈述不正确。该选项不能正确地工作，不应该使用。

### 5.1.3 IBM Tivoli Risk Manager 安装指南

应该更新附录 E『卸下组件』以包含以下信息：

在您卸载 Tivoli Risk Manager 组件之前请执行以下任务：

1. 关闭所有 Tivoli Risk Manager 适配器。
2. 发出 **wrmadmin -k** 命令以关闭 Tivoli Risk Manager 产品。
3. 如果您要卸下事件服务器，请执行以下任务：
  - a. 发出以下命令之一：  
对于 UNIX: **rmcorr\_cfg -delete**  
对于 Windows: **bash rmcorr\_cfg -delete**  
注：该命令执行以下操作：
    - 该命令装入缺省规则库。要使用定制的规则库，使用 GUI 或 **wrb** 命令手动将其装入。
    - 停止并重新启动 Tivoli Enterprise Console 事件服务器
  - b. 发出 **wrmadmin -k** 命令。
4. 卸载组件。有关您应该用于要卸下的组件的命令的信息，请参阅第 177 页的表 11。

注：

1. 已更改的 Tivoli Risk Manager 文件或已添加的适配器文件将不从 Tivoli Risk Manager 目录中删除。
2. 在事件服务器上，Tivoli Risk Manager 归档表、数据库视图以及事件控制台事件组在卸载过程中不删除。如果您想删除这些组件，则必须手动删除。

### 5.1.4 IBM Tivoli Risk Manager 问题确定指南

以下信息应添加到第 23 页的『Tivoli 管理环境发送连接类型』一节：

如果当重新安装 Tivoli Risk Manager 产品时传送类型更改为 TME，则 /etc/Tivoli/rma\_eif\_env.sh 脚本文件中 TMEEndpoint 关键字的值必须更改为 true，如下所示：

```
TMEEndpoint=true
```

## 5.2 队列管理和操作

本节提供有关已对 APAR IY55319 队列的操作和管理进行的增强的信息。已进行了这些更改以改进由持久队列使用的磁盘空间的管理。该更改之前，如果事件过长时间置于比处理这些事件更快的队列上，则 Tivoli Risk Manager 产品失败且不会将原因通知管理员。要解决该问题，已添加配置参数以管理队列并通知管理员关于队列的状态。有关这些更改的更多信息，请查看《IBM Tivoli Risk Manager 管理员指南》中对『队列和事件持久状态』一节的以下更改：

### 队列和事件持久状态

在 rmagent.xml 文件中引用为接口中的“to”设置的代理程序的每个子组件都具有与其处理关联的队列。子组件需要处理的事件由指定为接口中的“from”设置的子组件放置在关联的队列上。当准备处理事件就绪时，处理的子组件从队列删除事件。

#### 了解持久状态

持久状态受控于 rmagent.xml 文件中的 **persist** 参数。在缺省情况下，当放置在队列上时，事件持久保存到磁盘。当处理的子组件完成其任务时，该事件从磁盘删除。您可以将引擎和目标组件队列配置为不将事件持久保存到磁盘。在确定是否想持久保存事件之前，请仔细查看以下信息。

下表提供信息以帮助您了解事件持久状态：

描述	持久状态	无持久状态
所有事件写入磁盘	是	否
失败的事件写入磁盘	是	是
当代理程序停止时，队列事件写入磁盘（作为失败的重试事件）	否	是
当代理程序启动时，将处理失败的（重试）事件。	是	是
失败的（永久的）事件写入磁盘	是	是

#### 为什么关闭持久状态？

由于忽略将事件数据写入磁盘并稍后删除，处理可能更快。

#### 为何不关闭持久状态？

您的系统不具有可用于代理程序的无限制的内存。如果不将事件持久保存到磁盘，则必须将它们保持在内存中。即使意外错误条件导致代理程序终止，您也不想丢失事件。在持久状态关闭的情况下，您可能丢失事件数据。

#### 是否应该关闭持久状态？

不建议使用关闭持久状态的选项。强烈推荐您使用持久状态。

要关闭持久状态，请编辑 rmagent.xml 文件并将 **persist="no"** 添加到子组件定义中，例如：

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

</destination>

## 队列管理和控制参数

以下可选参数可以结合 `rmagent.xml` 配置文件中的 `<destination>` 元素使用来控制操作和管理队列：

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

队列的大小和可用磁盘空间的数量在事件将排队时评估。如果队列的大小接近由 **queueMaxSize** 和 **queueThresholdSize** 参数指定的大小，则 `RMAgent_QueueProblem` 事件将发送到由 **errorRoute** 参数指定的事件控制台。**queueMessageInterval** 参数控制队列警告事件发送的频率。如果没有要排队的事件或队列已处于等待状态之一，则队列大小和磁盘空间将不评估，且无队列警告事件生成。

以下信息提供每个参数的描述：

### **queueThresholdSize**

- 该参数指定在队列警告事件发送至事件控制台之前队列必须达到的大小。当初始达到该值且以由 **queueMessageInterval** 参数指定的时间间隔再发送至由 **errorRoute** 参数指定的事件控制台时，将发送第一个事件。
- 如果队列达到由该参数指定的大小时，它不停止处理该子组件的事件。
- 该参数的值可以是 0 和 2147483647 之间的整数。缺省值 0 表示没有大小限制。
- 当队列处于该状态时，它的状态是“正在运行（阈值）”，如 `wrmqueue -l` 命令显示。

### **queueMaxSize**

- 该参数指定队列可以包含的事件的最大个数。当队列中的事件数量接近值时，将事件发送至队列的组件停止处理且队列警告事件将发送至事件控制台。当初始达到该值且以由 **queueMessageInterval** 参数指定的时间间隔再发送至由 **errorRoute** 参数指定的事件控制台时，将发送第一个事件。缺省时间间隔是 15 分钟。
- 该参数的值可以是 0 和 2147483647 之间的整数。缺省值 0 表示没有大小限制。该参数的值必须大于 **queueThresholdSize** 参数值。
- 当队列达到最大大小时，它的状态是“正在等待（最大）”，如 `wrmqueue -l` 命令显示。

### **queueMessageInterval**

- 该参数指定在下一个 `RMAgent_QueueProblem` 队列警告事件发送之前的时间（以毫秒计）。当队列已超出由 **queueMaxSize** 或 **queueThresholdSize** 参数指定的大小时，使用该参数限制发送的队列警告事件的数量。
- 缺省值是 900000（15 分钟）。

### **errorRoute**

- 当超出 **queueMaxSize** 或 **queueThresholdSize** 参数值时，该参数指定队列警告事件发送到的组件（通常为事件控制台）。
- 队列警告事件与该路由的所有其它事件排在一起。使用该参数通过定义错误路由的单独目标地址来加速发送队列警告事件。这将确保队列警告事件以及及时的方式传递。

- 可以定义多个错误路由。RMAgent\_QueueProblem 队列警告事件将发送至所有指定的错误路由。
- 没有缺省的错误路由。如果该参数未指定，则无 RMAgent\_QueueProblem 队列警告事件发送。

### 使用队列管理和控制参数的示例

本节提供基于以下情况使用队列管理和控制参数的示例：

目的	使用的参数	示例
确保排队的事件的数量永不超出 100 000。	queueMaxSize	queueMaxSize = "100000"
当排队的事件数量达到 10 000 时，您想要队列警告事件发送。	queueThresholdSize	queueThresholdSize="10000"
您想要队列警告事件发送。	errorRoute	参阅以下示例。
您想要队列警告事件每分钟发送一次。	queueMessageInterval	queueMessageInterval="60000"

以下示例显示对于以上所列目的指定的所有队列参数：

```
<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\RISKMG\etc\error_route.conf"/>
</destination>
```

### 队列管理事件的示例

本节提供了队列管理事件的示例。请注意，仅显示部分事件。

- 以下事件通知您排队的事件数量已达到或超出由 **queueThresholdSize** 参数指定的配置的队列阈值大小。

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

- 以下事件通知您排队的事件数量接近或已超出由 **queueMaxSize** 参数指定的配置的队列最大大小。

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

- 以下事件通知您持久队列使用的硬盘驱动器没有更多的可用空间。

```
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
```

- 以下事件通知您队列已失败并需要手动干预。

```
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 命令描述

**wrmqueue** 命令的 **-l** 选项的描述在《*IBM Tivoli Risk Manager 命令参考大全*》中应更改如下：

### l 或 -list

该选项列出有关队列的信息。该输出在三个部分中都有显示并按所列顺序提供以下信息：

1. 队列名、状态和定义
2. 队列中事件的数量
3. 失败事件的数量

以下输出是 **wrmqueue -l** 输出的示例：

队列名	状态	类型	持久
summarization	正在运行	引擎	是
EIF_sender1	正在等待（最大）	发送器	是
EIF_sender2	正在运行（阈值）	发送器	否
EIF_sender3	正在等待（磁盘已满）	发送器	是
EIF_sender4	已失败	发送器	否

  

队列名	# 已排队	# 已处理	#/秒
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

  

队列名	# 已失败
summarization	ttttttttt(rrrrrrrrr)
EIF_sender1	ttttttttt(rrrrrrrrr)
EIF_sender2	ttttttttt(rrrrrrrrr)
EIF_sender3	ttttttttt(rrrrrrrrr)
EIF_sender4	ttttttttt(rrrrrrrrr)

以下信息描述了由 **wrmqueue** 命令的 **-l** 选项提供的输出：

列标题	信息描述
队列名	队列的名称。
状态	队列的状态（非组件）。通过以下值之一表示状态：

	正在运行 正在等待（最大）  正在运行（阈值） 正在等待（磁盘已满）  已失败	队列运行无问题。 已配置的最大队列大小已达到，且正将事件发送至该队列的任何组件均置于等待状态。 已配置的阈值队列大小已超出。 存储 <b>Tivoli Risk Manager</b> 持久文件的磁盘已满，且代理程序正在等待直到空间可用。 队列已失败。有关解决该问题的信息，请参阅《 <i>Tivoli Risk Manager 问题确定指南</i> 》。
类型	正从该队列读取事件的组件类型： <ul style="list-style-type: none"> <li>引擎</li> <li>发送器</li> </ul>	
持久状态	表示事件是存储在内存中还是存储在硬盘上。	
# 已排队	组件可用的要处理的事件数量。	
# 已处理	自代理程序上一次启动以来成功处理的事件数量。	
#/秒	自上一次 <b>wrmqueue -l</b> 命令发出或代理程序重新启动后（如果这是首次发出 <b>wrmqueue -l</b> 命令）以来每秒处理的事件数量。	
# 已失败	<b>tttttttt</b> 是自代理程序上一次启动以来组件已无法处理的事件总数。 <b>rrrrrrrr</b> 是代理程序重新启动时将重试的失败队列尝试的数量。	

## 5.3 消息和跟踪日志

本节提供有关新的第一次失败数据捕获（FFDC）功能以及对《*IBM Tivoli Risk Manager 问题确定指南*》的第二章『消息和跟踪日志及其它诊断工具』的其它更改的信息。

### 跟踪日志

**Tivoli Risk Manager** 产品提供跟踪详细信息的三个级别。详细信息的最低级别（**DEBUG\_MIN**）是缺省级别。在该级别，仅跟踪错误条件。下两个级别是 **DEBUG\_MID** 和 **DEBUG\_MAX**，它们提供更大量的详细信息。可以通过更改日志配置文件中的参数或通过调用日志命令行界面来修改级别。跟踪日志数据当前仅英语可用。

在缺省情况下，内存缓冲区用于存储所有跟踪信息。这最小化了系统性能上跟踪的影响。仅当异常发生时缓冲区清空至磁盘。您还可以配置跟踪日志以直接写入磁盘，以便当无异常发生时您可以存储跟踪数据。有关如何配置跟踪日志的示例，请参阅『*Tivoli Risk Manager* 代理程序和事件监视器跟踪定制』一节。

跟踪日志位于以下文件和目录中：

- Linux 和 UNIX 系统上的 **Tivoli Risk Manager C** 程序跟踪日志位于 `/usr/ibm/tivoli/common/HRM/logs/<application>.error.log` 中。变量 `<application>` 指定应用程序的名称。
- Windows 系统上的 **Tivoli Risk Manager C** 程序跟踪日志位于 `C:\Program Files\ibm\tivoli\common\HRM logs\<application>.error.log` 中。变量 `<application>` 指定应用程序的名称。
- 对于 Linux 和 UNIX 系统的 **Tivoli Risk Manager** 代理程序组件跟踪日志位于 `/usr/ibm/tivoli/common/HRM/logs/traceHRMn.log` 中。
- 对于 Windows 系统的 **Tivoli Risk Manager** 代理程序组件跟踪日志位于 `C:\Program Files\ibm\tivoli\common\HRM logs\traceHRMn.log` 中。

- Tivoli Risk Manager 数据库实用程序、wrmdbclose 和 wrmdbclear 将它们的跟踪记录分别地写到单独文件：traceHRM\_DBClose.log 和 traceHRM\_DBClear.log。

Tivoli Risk Manager 代理程序和事件监视器跟踪记录将写到名为 traceHRMn.log（其中 *n* 是一个数字）的按顺序编号的文件中。跟踪记录器可以最多写 5 个文件，每个大小为 1 MB。如果写入了比可以满足 5 MB 更多的跟踪记录，则跟踪文件将合并。这些跟踪文件限制都可以使用记录器配置文件定制。要更改跟踪文件的编号，使用 **file.trace.maxFiles** 参数。要更改每个跟踪文件的最大大小，使用 **file.trace.maxFileSize** 参数。

大多数日志消息同时写到消息日志和跟踪日志。要确保所有消息都写到跟踪日志，将跟踪文件添加到消息记录器的 listenerNames，如下所示：

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

### 第一次失败数据捕获

第一次失败数据捕获（FFDC）是在错误条件时跟踪信息的快照。通过定制跟踪日志配置，您可以使跟踪快照在所有错误或选定错误下进行。每个快照创建唯一的跟踪文件，该文件不会被后继跟踪快照覆盖。在缺省情况下，FFDC 在 Tivoli Risk Manager 产品中不活动。可以通过更改跟踪日志配置将其激活。有关更改配置的信息，请参阅『Tivoli Risk Manager 代理程序和事件监视器跟踪定制』一节。

FFDC 快照仅对于 Tivoli Risk Manager 代理程序和事件监视器可用。

FFDC 日志位于以下文件和目录中：

在 UNIX 系统上：/usr/ibm/tivoli/common/HRM/FFDC/YYYY.MM.DD/traceHRMn.log

在 Windows 系统上：C:\Program Files\ibm\tivoli\common\HRM FFDC\YYYY.MM.DD\traceHRMn.log

变量 YYYY.MM.DD 是快照发生的日期，且 *n* 是一个表示在给定日期快照的顺序的数字。

### 日志 XML

以下几列消息和跟踪日志记录由 Tivoli Risk Manager 产品使用：

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

示例

以下查询以 ASCII 显示消息日志文件的内容：

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

以下查询以 HTML 将跟踪日志文件的内容写入外部文件：

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

以下查询以 HTML 格式将跟踪日志文件的选定列写入外部文件：

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

以下查询以 HTML 格式将“错误”消息的选定列从消息日志文件写入外部文件：

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

## Tivoli Risk Manager 代理程序和事件监视器跟踪定制

Tivoli Risk Manager 代理程序跟踪日志由 `$RMADHOME/etc/RMLogger.properties` 跟踪日志配置文件中的参数控制。例如，**rmLogger.trc.level** 参数控制代理程序运行时收集的跟踪信息的数量。

**rmLogger.trc.listenerNames** 参数控制将跟踪信息写入内存还是写入磁盘上的文件。要增加代理程序执行的跟踪日志的数量，通常这两个参数都必须更改以便有更多的信息捕获并在创建时写入磁盘。

有两种方法可对跟踪配置进行更改：

- 通过更改 `RMLogger.properties` 文件中的参数值然后重新启动代理程序的永久方法

例如，使用以下步骤永久地增加代理程序跟踪日志：

1. 编辑 `$RMADHOME/etc/RMLogger.properties` 文件以更改以下参数：  
    `rmLogger.trc.level=DEBUG_MAX`  
    `rmLogger.trc.listenerNames=file.trace`
2. 重新启动代理程序。

- 通过使用日志命令行界面（请参阅『日志命令行界面』一节）更改参数值的临时的方法。  
通过该方法进行的更改需要代理程序正在运行，且仅当代理程序正在运行时有效。

例如，使用以下步骤当代理程序正在运行时临时增加代理程序跟踪日志。

1. 更改为 `$RMADHOME/logviewer` 目录。
2. 从该目录输入以下命令：  
    `logcmd set rmLogger.trc level=DEBUG_MAX`  
    `logcmd set rmLogger.trc listenerNames=file.trace`

当记录更多信息时跟踪日志变得更大。在已达到跟踪文件的最大数量之后，原有跟踪数据将被新的数据覆盖。缺省跟踪配置是 5 个跟踪文件，每个 1 MB。要将跟踪文件容量增加为 10 个文件，每个 2 MB，请发出以下命令：

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

这些设置只要在代理程序运行时就保持生效；停止和重新启动代理程序将导致这些设置返回到其缺省设置。要减少代理程序运行时代理程序跟踪日志，请发出以下命令：

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

要启用第一次失败数据捕获（FFDC）快照，请如下定制跟踪配置：

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

所有这些配置更改影响 Tivoli Risk Manager 代理程序的所有组件，包括事件监视器。如果您想配置事件监视器使其不同于其余的代理程序，则在配置文件或命令行界面中使用 **rmLogger.trc.monitor** 代替 **rmLogger.trc**。例如，要将事件监视器跟踪日志设置为中级别并写入它自己的文件，请设置以下参数：

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

发出以下命令以列出配置中所有定义的跟踪记录器：

```
logcmd list rmLogger.trc
```

发出以下命令以列出跟踪记录器的当前设置：

```
logcmd config rmLogger.trc
```

发出以下命令以列出事件监视器跟踪记录器的当前设置：

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

## 5.4 正则表达式支持

本节提供有关对 **APAR IY53527** 的正则表达式支持进行的增强的信息。以下有关使用正则表达式的信息应添加到《*IBM Tivoli Risk Manager 管理员指南*》：

### 正则表达式支持

在 **IBM Tivoli Risk Manager V4.2** 中，以下新的功能将添加到依赖于正则表达式支持 **Tivoli Risk Manager** 产品的介绍的事件监视器。

- 预过滤
- 建立索引
- 对于指定事件模式的增强功能

该新功能改进总体的性能，并简化格式文件的创建。除了前发行版中提供的简单通配符标记之外，您现在可以在格式文件中将事件模式表示为正则表达式。

要实现这些新功能，使用从 **Xerces** 的正则表达式库。 **Xerces** 正则表达式匹配引擎是传统（非 **POSIX**）不确定有限自动监视器（**NFA** 正则表达式引擎的一项实现。该库支持大多数受支持的正则表达式构成部分，如下所示：

构成	符号	描述	示例	结果
简单字符类	[ ]	字符类（或字符集）的基本格式。使用该构成部分仅匹配若干字符中的一个。	gr[ae]y	匹配“gray”或“grey”。
求反的字符类	[ ^ ]	匹配所有字符（除所列之外）。在打开的方括号后输入插入标记来抵消字符类。	gr[^ae]y	既不匹配“gray”也不匹配“grey”。
重复字符	? * +	匹配先行的标记零次或一次。 匹配先行的标记零次或多次。 匹配先行的标记一次或多次。		
速记字符	\d \D \s \S \w \W	匹配任何数字 匹配任何非数字 匹配任何空格字符 匹配任何非空格字符 匹配任何字符： 匹配任何非字符：		
点	[.]	匹配几乎任何字符。当使用该构成部分时请小心。点（或句号）是最常用的元字符之一，它也是最常误用的元字符。		
定位符		用于表示位置，不匹配字符。它们在字符之前、之后或之间匹配位置，并用于在某些位置标记 <b>regex</b> 匹配。		

	^ \$	表示一行的开始。 表示一行的结束。		
字边界	\b \B \w \W	表示字边界。 用于匹配整个字。 \b 的求反版本。 用于匹配非字符。 \w 的求反版本。	\b(is art)\b	匹配字“is”或字“art”。
范围	[ ]	用于指定值的范围。 请注意，您在字符类内指定多个范围或者甚至组合范围和单个字符。	[0-9]  [0-9a-fxA-FX]	匹配 0 和 9 之间的单个数字。 匹配十六进制数字或字母 X。
量词	{ }	使用量词以进一步确定表达式的数量。 ?、* 和 + 也是量词。	{n}  {n,}  {n,m}	严格匹配 <i>n</i> 次。 匹配至少 <i>n</i> 次。 匹配至少 <i>n</i> 次， 但不多于 <i>m</i> 次。
向前看	(?=) (?!)	匹配下一个字符。	q(?=u)  q(?!u)	匹配随后是 u 的 q。 匹配随后不是 u 的 q。
向后看	(?<=)	匹配上一个字符	(?<=a)b  (?<!a)b	匹配上一个字母是 a 的字母 b。 匹配上一个字母不是 a 的字母 b。
分组的交替	(a e) gr[ae]y	匹配给定若干可能的表达式的单个正则表达式。  请注意，如果在表达式开始或结束指定“( and )”，则 匹配不能正确地实现。  这是由于 Xerces 库的问题所导致。	gr(a e)y gr[ae]y (gray grey)	匹配“gray”或“grey”。

下表列出了不受支持的构成部分以及可以使用的备用构成部分。

构成部分	描述	备用构成部分
并集	指定由两个或多个单独的字符类构成的单个字符类。并集的示例可以为 [0-4[6-8]]，它应匹配除 5 以外从 0 到 8 的任何数字。	指定 [0-46-8]，它避免了嵌套方括号且可以达到相同的结果。
交集	指定匹配所有公共内容的单个字符类。交集的示例为 [0-4&&[4678]]，它将匹配数字 4。交集类似于并集，且在类似的环境中使用。	使用与并集指定的相同的备用构成部分。
减法	指定匹配除公共以外所有内容的单个字符类。减法实质上是求反的交集。减法的示例是 [0-9&&[^345]]，它将匹配除 3、4 和 5 以外从 0 到 9 的任何数字。	以正数格式指定表达式。例如，[0-26-9]。



## 6 添加或替换的文件

本节列出了该修订包的新的和更改的文件。RMADHOME 涉及 Tivoli Risk Manager 安装目录（由 RMADHOME 环境变量引用）。

```
/etc/init.d/rc.rmagent (Solaris 和 Linux)
/etc/rc.rmagent (AIX)
/etc/Tivoli/rma_eif_env.sh (删除 SUSE Linux V8 及更高版本上的 LD_ASSUME_KERNEL)
RMADHOME/bin/rma_webids-init (仅 UNIX 或 Linux)
RMADHOME/bin/RMCAH040201.sys (仅 HPUX)
RMADHOME/bin/RMCAL040201.sys (仅 Linux)
RMADHOME/bin/RMCAS040201.sys (仅 Solaris)
RMADHOME/bin/RMCAW040201.sys (仅 Windows)
RMADHOME/bin/RMCAX040201.sys (仅 AIX)
RMADHOME/bin/rmEventLog.dll (仅 Windows)
RMADHOME/bin/webids[.bat]
RMADHOME/bin/wrmadmin[.exe]
RMADHOME/bin/wrmdns (除 Windows 和 Solaris 以外的全部)
RMADHOME/bin/wrmqueue (除 Windows 和 Solaris 以外的全部)
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 (仅 UNIX 或 Linux)
RMADHOME/logviewer/logcmd.bat (仅 Windows)
RMADHOME/msg_cat/C/rmeif.cat
RMADHOME/nids/templates/rules/www.rules
RMADHOME/reports/rm_ra_03.rpt (仅 Windows)
\Program Files\ibm\tivoli\common\HRM\scripts/getpd.bat (仅 Windows)
\Program Files\ibm\tivoli\common\HRM\scripts/getpdinfo.bat (仅 Windows)
/sbin/init.d/rc.rmagent (HP)
/usr/ibm/tivoli/common/HRM/scripts/getpdinfo (仅 UNIX 或 Linux)
```



## 7 联系软件支持

如果您有关于任何 Tivoli 产品的问题，请参阅以下 IBM 软件支持 Web 站点：

<http://www.ibm.com/software/sysmgmt/products/support/>

如果您想联系软件支持，请参阅位于以下 Web 站点的 IBM 软件支持指南：

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

该指南提供有关如何根据您问题的严重性联系 IBM 软件支持的信息以及以下信息：

- 注册和资格
- 电话号码和电子邮件地址（取决于您所在的国家或地区）
- 在联系 IBM 软件支持之前您必须具有的信息



## 8 声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往：

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

有关双字节（DBCS）信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

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

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区：**International Business Machines Corporation**“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品和 / 或程序进行改进和 / 或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：（i）允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与下列地址联系：

IBM Corporation  
224A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此

外，有些测量是通过推算而估计的，实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 **IBM** 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。**IBM** 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 **IBM** 产品的声明。有关非 **IBM** 产品性能的问题应当向这些产品的供应商提出。

所有关于 **IBM** 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

本信息包含日常业务经营中使用的数据和报告的示例。要尽可能完整地对其进行说明，示例包含个人、公司、品牌和产品的名称。所有这些名称都是虚构的，且任何类似于由实际企业使用的名称和地址都纯属巧合。

版权许可：

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（**API**）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 **IBM** 付费。这些示例并未在所有条件下作全面测试。因此，**IBM** 不能担保或暗示这些程序的可靠性、可维护性或功能。用户如果是为了按照 **IBM** 应用程序编程接口开发、使用、经销或分发应用程序，则可以任何形式复制、修改和分发这些样本程序，而无须向 **IBM** 付费。

如果您正以软拷贝格式查看本信息，图片和彩色图例可能无法显示。

## 商标

以下术语是 **International Business Machines Corporation** 在美国和 / 或其他国家或地区的商标：

**IBM**、**IBM** 徽标、**Tivoli**、**Tivoli** 徽标、**AIX**、**DB2**、**Tivoli Enterprise Console**、**TME**、**pSeries** 和 **zSeries** 是 **International Business Machines Corporation** 或 **Tivoli Systems Inc.** 在美国和 / 或其他国家或地区的商标或注册商标。

**Linux** 是 **Linus Torvalds** 在美国和 / 或其他国家或地区的商标。

**Microsoft** 和 **Windows** 是 **Microsoft Corporation** 在美国和 / 或其他国家或地区的注册商标。

**UNIX** 是 **The Open Group** 在美国和其他国家或地区的注册商标。



Java 和所有基于 Java 的商标是 **Sun Microsystems, Inc.** 在美国和 / 或其他国家或地区的商标。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

