o

IBM Tivoli Risk Manager
Versione 4.2 Fix Pack 1
File Readme

Nota:

Prima di utilizzare queste informazioni e il prodotto ad esse collegato, leggere la sezione Informazioni particolari, alla pagina 34.

Prima edizione (settembre 2004)

Questa edizione riguarda IBM Tivoli Risk Manager, Versione 4.2, fix pack 1 e tutti i successivi rilasci e modifiche, se non diversamente indicato nelle nuove edizioni.

© Copyright International Business Machines Corporation 2004. Tutti i diritti riservati.

Limitazioni previste per gli utenti appartenenti al Governo degli Stati Uniti - L'uso, la duplicazione o la divulgazione sono limitati dal GSA ADP Schedule Contract con IBM Corp.

Sommario

1 Informazioni su questo fix pack ... 3
1.1 Contenuto del fix pack ... 3
1.2 Patch sostituite da questo fix pack ... 3
1.3 Sistemi operativi supportati ... 3
1.4 Novità di questo fix pack ... 4

2 Installazione e configurazione ... 5
2.1 Prerequisiti ... 5
2.2 Note di installazione ... 5
2.3 Istruzioni per l'installazione ... 7
2.3.1 Installazione di patch ... 7
2.4 Informazioni sul pacchetto di localizzazione ... 8
2.4.1 Note sul pacchetto di localizzazione ... 8
2.4.2 Istruzioni per l'installazione del pacchetto di localizzazione ... 8
2.4.2.1 Installazione completa ... 8
2.4.2.2 Installazione di patch ... 8

3 APAR corretti da questo fix pack ... 9

4 Limitazioni note ... 12
4.1 Installazione ... 12
4.2 Server di correlazione ... 12
4.3 Server eventi Tivoli Enterprise Console ... 12
4.4 Agente Tivoli Risk Manager ... 13
4.5 Risoluzione DNS ... 14
4.6 Registrazione di messaggi e tracce ... 14
4.7 Componente Network IDS ... 15
4.8 Componente Web IDS ... 15
4.9 Applicazione Web ... 15

5 Aggiornamenti della documentazione ... 17
5.1 Correzioni relative a varie documentazioni ... 17
5.1.1 IBM Tivoli Risk Manager Administrator's Guide ... 17
5.1.2 IBM Tivoli Risk Manager Command Reference ... 19
5.1.3 IBM Tivoli Risk Manager Installation Guide ... 19
5.1.4 IBM Tivoli Risk Manager Problem Determination Guide ... 20
5.2 Funzionamento e gestione delle code ... 20
5.3 Registrazione di messaggi e traccia ... 25
5.4 Supporto espressioni regolari ... 28

6 File aggiunti o sostituiti ... 31

7 Come contattare il supporto software ... 32

8 Informazioni particolari ... 34

1 Informazioni su questo fix pack

Questa sezione fornisce informazioni generali su questo fix pack. Prima di installare questo fix pack, leggere l'intero documento.

Questo readme è fornito solo in formato Adobe Acrobat.

Per informazioni sul pacchetto di localizzazione fornito con questo fix pack, consultare la sezione *Informazioni sul pacchetto di localizzazione* di questo file readme.

1.1 Contenuto del fix pack

Questo fix pack contiene:

?? Questo file readme

?? Un report per questo fix pack

?? Il CD-ROM di questo fix pack

1.2 Patch sostituite da questo fix pack

Le seguenti patch sono sostituite da questo fix pack:

?? 4.2-RMG-0001LA

?? 4.2-RMG-0002LA

?? 4.2-RMG-0003LA

?? 4.2-RMG-0004LA

1.3 Sistemi operativi supportati

La sezione elenca le piattaforme e i database supportati da questo fix pack.

Versioni del sistema operativo supportato [1]	**Ruoli**				**Componenti opzionali**			
	Server eventi	**Server di correlazione distribuito**	**Gateway**	**Client**	**Crystal Reports**	**Network IDS**	**Web IDS**	**Applicazione Web**
AIX® 5L V5.1 (32 bit o 64bit)	X	X	X	X		X[3]	X	X
AIX 5.L V5.2 (32 bit o 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 o 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
Red Hat Enterprise Linux AS 3.0 (IA32)	X	X	X	X		X		

Versioni del sistema operativo supportato [1]	Ruoli				Componenti opzionali			
	Server eventi	Server di correlazione distribuito	Gateway	Client	Crystal Reports	Network IDS	Web IDS	Applicazione Web
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

Note sul sistema operativo:

1. Le informazioni contenute in questa tabella sono basate su dati disponibili al momento della creazione di questo fix pack. La tabella fa riferimento a sistemi operativi non obsoleti, come indicato dal fornitore del sistema operativo. Per informazioni sul supporto corrente, fare riferimento al supporto in linea IBM.
2. Solaris si riferisce all'ambiente operativo Solaris, d'ora in avanti indicato come Solaris.
3. Network IDS (Network Intrusion Detection System) non è supportato da sistemi a 64 bit.

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

1.4 Novità di questo fix pack

La sezione fornisce informazioni sulle modifiche effettuate al prodotto Tivoli Risk Manager.

?? Il supporto per la gestione delle code è stato migliorato. Attualmente sono disponibili parole chiave che forniscono uno strumento per controllare la dimensione delle code e inviare eventi sullo stato della coda. Per ulteriori informazioni, consultare la sezione Aggiornamenti della documentazione.

?? Il supporto delle espressioni regolari è stato migliorato. Attualmente viene utilizzata una libreria più consistente e aggiornata della libreria di espressioni regolari Xerces, che fornisce un più ampio supporto per la sintassi delle espressioni regolari standard. Per ulteriori informazioni, consultare la sezione Aggiornamenti della documentazione.

?? È stato aggiunto il supporto della funzione FFDC (First Failure Data Capture). Per ulteriori informazioni, consultare la sezione Aggiornamenti della documentazione.

?? L'attributo msg incluso nell'evento RMAgent_Inactive è stato ampliato in modo da comprendere il nome host e l'indirizzo IP dell'agente che non invia più eventi RMAgent_HeartBeat. Per ulteriori informazioni, consultare la sezione Aggiornamenti della documentazione.

?? Attualmente è fornito il supporto per Windows 2003 Server.

2 Installazione e configurazione

2.1 Prerequisiti

Per Tivoli Risk Manger fix pack 1 è richiesto il seguente software:

- ?? IBM Tivoli Risk Manager, Versione 4.2
- ?? IBM Tivoli Enterprise Console, Versione 3.9 con FP01 (solo per il ruolo server eventi).
- ?? Per Red Hat Enterprise Linux, la versione di runtime Java raccomandata è IBM JRE 1.3.1-6 o successiva. Se non è possibile utilizzare queste versioni, contattare il supporto software IBM.

2.2 Note di installazione

Questa sezione fornisce informazioni aggiuntive sull'installazione del prodotto Tivoli Risk Manager.

- ?? Se è stato installato il fix pack Tivoli Risk Manager 4.2.0-RMG-FP01 e si desidera installare un componente opzionale (ad esempio Crystal Reports) che non è stato installato durante la procedura di installazione iniziale di Tivoli Risk Manager, contattare il Supporto Software IBM per il fix pack di installazione richiesto per eseguire tale procedura.
- ?? Questo fix pack può essere utilizzato per un'installazione completa o per l'installazione di patch. Per ulteriori informazioni sul metodo da utilizzare, consultare la sezione Istruzioni per l'installazione.
- ?? Il monitor eventi di Windows crea chiavi di registro che indicano l'ultima posizione in cui sono stati letti i registri eventi di Windows. Queste voci sono utilizzate per determinare il punto di inizio della lettura quando viene riavviato il monitor eventi o l'agente Tivoli Risk Manager. Quando il prodotto Tivoli Risk Manager viene disinstallato, il programma di disinstallazione non rimuove tali chiavi di registro dal registro. Se viene reinstallato il monitor eventi, le vecchie chiavi di registro sono utilizzate al primo riavvio del monitor eventi, che inizia a leggere i vecchi eventi.
  Per assicurarsi che all'avvio il monitor eventi di Windows legga a partire dalla data corrente, e non legga eventi precedenti, eliminare la seguente chiave di registro del monitor eventi prima di avviarlo per la prima volta: HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Riskmgr\Agent\RMLogfile
- ?? L'installazione dell'applicazione Web di Tivoli Risk Manager su un sistema Solaris potrebbe essere molto lenta o addirittura arrestarsi. Il numero massimo predefinito di file aperti potrebbe essere impostato su un valore troppo piccolo per cui WebSphere Application Server potrebbe non essere in grado di installare il componente dell'applicazione Web di Tivoli. Per questo motivo WebSphere Application Server potrebbe ritentare continuamente l'installazione invece di restituire un codice di errore.
  È possibile determinare il limite del descrittore file immettendo il seguente comando:

  ulimit -n

  Per installare il componente applicazione Web di Tivoli Risk Manager su WebShpere Application Server, quest'ultimo deve esser avviato con un descrittore file massimo non inferiore a 1024 (presumendo che le applicazioni WebSphere Application Server di esempio siano state installate con l'applicazione Web Tivoli Enterprise Console), prima di installare l'applicazione Web Tivoli Risk Manager utilizzando una delle seguenti procedure. Prima di procedere, tuttavia, consultare la documentazione di Solaris per conoscere precauzioni, esecuzione e conseguenze di queste modifiche. Potrebbe essere necessario modificare il valore esatto del descrittore file massimo a seconda del numero di applicazioni WebSphere Application Server installate.

  Per modificare il descrittore file massimo, utilizzare uno dei seguenti metodi:

  1. Arrestare WebSphere Application Server.
  2. Immettere il seguente comando:
     ulimit -n 1024
  3. Riavviare WebSphere Application Server dalla stessa sessione comandi in cui il comando **ulimit** è stato immesso.
  4. Installare il prodotto Tivoli Risk Manager.

Una soluzione definitiva consiste nel modificare i valori di sistema relativi ai descrittori file impostando i seguenti attributi nel file /etc/system:

```
rlim_fd_cur
rlim_fd_max
```

?? Per una nuova installazione del prodotto Tivoli Risk Manager con un database Sybase, la tabella Tivoli Risk Manager viene installata nel segmento predefinito del database del prodotto Tivoli Enterprise Console. Il segmento predefinito definito dall'installazione di Tivoli Enterprise Console è molto piccolo, per cui contiene solo un numero molto limitato di eventi della tabella archivio di Tivoli Risk Manager. Per utilizzare su Sybase il prodotto Tivoli Risk Manager con l'implementazione predefinita, il segmento predefinito del database di Tivoli Enterprise Console può essere incrementato aggiungendo un altro dispositivo.

La seguente procedura fornisce un esempio di come aumentare la grandezza del segmento predefinito creando un dispositivo da 200 MB nel segmento predefinito denominato TEC_SYSTEM_2.

Note:

- ?? L'istruzione ALTER DATABASE aggiunge automaticamente un nuovo dispositivo al segmento predefinito.
- ?? Per eseguire questa procedura, utilizzare l'ID utente del sistema Sybase per impostare l'ambiente Sybase. Tale ID utente deve avere l'autorità appropriata e appartenere all'ambiente Sybase.

1. Creare uno script con nome file rm_exp_archive_table.syb.sql come di seguito descritto:

```
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. Valutare i seguenti parametri e modificarli a seconda delle esigenze di installazione:
   - ?? **DISK INIT** name: scegliere un nome appropriato per l'installazione.
   - ?? **physname**: specificare il percorso del sistema operativo per il dispositivo da creare.
   - ?? **vdevno**: assicurarsi che sia un numero non utilizzato. Utilizzare il seguente comando per stabilire i numeri attualmente utilizzati: select distinct low/16777216 from sysdevices
3. Immettere il seguente comando per eseguire lo script:

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

   La variabile <*pw*> è la password di SQL e la variabile <*sistema*> è il nome del sistema su cui è installato il database.

?? Durante l'installazione viene visualizzato il seguente messaggio per indicare che non è stato possibile trovare l'eseguibile Java:

```
"JVM not found"
```

Tale problema potrebbe essere causato da spazio insufficiente nel filesystem che contiene la directory temporanea. In tal caso, è possibile eseguire una delle seguenti operazioni:

- ?? Liberare spazio nel filesystem
- ?? Allocare più spazio nel filesystem

Lo spazio richiesto potrebbe essere più del triplo delle dimensioni del JRE Java installato.

?? In caso di reinstallazione del prodotto Tivoli Risk Manager e di modifica del tipo di trasporto in TME, modificare il valore della parola chiave **TMEEndpoint** in true nel file di script /etc/Tivoli/rma_eif_env.sh come di seguito descritto:

```
TMEEndpoint=true
```

2.3 Istruzioni per l'installazione

Questa sezione fornisce informazioni sull'installazione di questo fix pack.

Il fix pack Tivoli Risk Manager 4.2.0-RMG-FP01 può essere utilizzato per un'installazione completa o per l'installazione di patch. L'installazione completa può essere eseguita alle seguenti condizioni:

?? Utilizzo di un'applicazione Web con qualsiasi prodotto RDBMS ad eccezione di DB2.

?? Installazione di questo fix pack su una delle seguenti piattaforme:

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)

Per conoscere il pacchetto d'installazione da utilizzare per un'installazione completa, contattare il Supporto Software IBM.

2.3.1 Installazione di patch

Per installare la patch immettere il seguente comando:

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

Per <*piattaforma*>, specificare una delle seguenti piattaforme:

aix:	Versioni di AIX supportate dal prodotto Tivoli Risk Manager
hpux:	Versioni di HP-UX supportate dal prodotto Tivoli Risk Manager
linux:	Versioni di Linux (IA32) supportate dal prodotto Tivoli Risk Manager
linuxppc:	Versioni di Linux (PPC) supportate dal prodotto Tivoli Risk Manager
solaris:	Versioni di Solaris (SPARC) supportate dal prodotto Tivoli Risk Manager
win:	Versioni di Windows supportate dal prodotto Tivoli Risk Manager

È possibile specificare una delle seguenti opzioni:

-silent	Tale opzione non richiede input da parte dell'utente. Per stabilire se l'installazione è riuscita, verificare che nel file di registro della directory di installazione il codice di ritorno abbia un valore diverso da zero.
-console	Questa opzione fornisce un'installazione terminale (modalità testo). Tenere presente che tale opzione non è disponibile su piattaforme Windows.

Se non viene specificata alcuna opzione, vengono visualizzate le seguenti finestre:

?? Language

?? Benvenuti

?? Pre-installation

?? Post-installation

Per tali finestre non è richiesto alcun input da parte dell'utente. Fare clic su **Avanti** quando viene visualizzata ciascuna finestra.

Se è stato installato questo fix pack sul server eventi, effettuare la seguente procedura prima di terminare l'installazione:

1. Assicurarsi che la rule base da utilizzare sia quella corrente.
2. Immettere il seguente comando:
   rmcorr_cfg -update

Nota: questo comando aggiorna la rule base e arresta e riavvia il server eventi di Tivoli Enterprise Console.

2.4 Informazioni sul pacchetto di localizzazione

I pacchetti di localizzazione inclusi nel fix pack 4.2-RMG-FP01 contengono traduzioni in tutte le lingue supportate dalla versione 4.2 del prodotto Tivoli Risk Manager. Questa sezione fornisce le seguenti informazioni sul pacchetto di localizzazione:

?? Note sul pacchetto di localizzazione.

?? Istruzioni per l'installazione del pacchetto di localizzazione

2.4.1 Note sul pacchetto di localizzazione

Esaminare le informazioni contenute in questa sezione prima di installare il fix pack 4.2-RMG-FP01.

?? Le risorse lingue internazionali aggiornate incluse in questo fix pack riflettono modifiche apportate all'interfaccia utente e ai messaggi di Tivoli Risk Manager.

?? Le differenze tra installazione completa e installazione di patch risiedono nel numero di file installati e nelle verifiche dei prerequisiti eseguite prima dell'installazione.

?? Le finestre visualizzate durante l'installazione di patch sono uguali a quelle visualizzate durante l'installazione completa.

2.4.2 Istruzioni per l'installazione del pacchetto di localizzazione

Questa sezione fornisce informazioni per l'installazione del pacchetto di localizzazione. I pacchetti di localizzazione per Tivoli Risk Manager, Versione 4.2, fix pack 01, possono essere utilizzati per un'installazione completa o per l'installazione di patch. Utilizzare l'installazione completa per eseguire un'installazione completa del prodotto base (per ulteriori informazioni fare riferimento alla sezione Istruzioni per l'installazione sopra riportata). Utilizzare l'installazione di patch per eseguire un'installazione di patch del prodotto base.

2.4.2.1 Installazione completa

Per eseguire un'installazione completa delle risorse lingue internazionali, consultare le istruzioni di installazione contenute nella sezione International Language Support di *IBM Tivoli Risk Manager Release Note*, Versione 4.2.

2.4.2.2 Installazione di patch

Per eseguire un'installazione di patch immettere uno dei seguenti comandi:

Per piattaforme Windows:

```
rmlp4201_setupwin32.exe
```

Per piattaforme UNIX e Linux:

./rmlp4201_setup <*piattaforma*> .bin

Per <*piattaforma*>, specificare una delle seguenti piattaforme:

aix:	Versioni di AIX supportate dal prodotto Tivoli Risk Manager
hp11x:	Versioni di HP-UX supportate dal prodotto Tivoli Risk Manager
linux:	Versioni di Linux (IA32) supportate dal prodotto Tivoli Risk Manager
linuxppc:	Versioni di Linux (PPC) supportate dal prodotto Tivoli Risk Manager
solaris:	Versioni di Solaris (SPARC) supportate dal prodotto Tivoli Risk Manager

Per Linux per zSeries (S/390):

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

3 APAR corretti da questo fix pack

Questa sezione fornisce una descrizione e la soluzione delle fix APAR fornite dal fix pack 4.2.0-RMG-FP01.

APAR: IY48016

Problema: quando più istanze di Web IDS (Web Intrusion Detection System) sono in esecuzione sullo stesso sistema, la funzione di ripresa non viene eseguita correttamente perché tutte le istanze utilizzano la stessa copia del file webids.lastread.

Soluzione: ogni istanza della funzione Web IDS attualmente utilizza la propria copia del file webids.lastread.

APAR: IY50483

Problema: su Tivoli Risk Manager o su Tivoli Enterprise Console Server il processo tec_rule comporta un utilizzo massiccio della CPU. Per tale motivo, gli eventi in arrivo rimangono in stato QUEUED.

Soluzione: Tivoli Enterprise Console di Tivoli Risk Manager controlla le modifiche durante la generazione di gruppi di incidenti per migliorare le prestazioni. Sono state aggiunte ulteriori opzioni di configurazione per l'elaborazione di gruppi di incidenti nel file riskmgr_config.pro della directory $RMADHOME/etc/tec/rules. Per ulteriori informazioni sull'utilizzo di queste opzioni, consultare i commenti contenuti nel file riskmgr_config.pro.

APAR: IY52322

Problema: il server di correlazione distribuito si arresta quando riceve un evento parziale.

Soluzione: una nuova parola chiave API di Tivoli Enterprise Console, **ReadRetryInterval**, viene utilizzata per configurare il valore del timeout utilizzato dall'API Event Integration Facility quando viene ricevuto un evento parziale.

Il valore predefinito di questa parola chiave è di 120 secondi.

Quando il sender di Event Integration Facility gestisce eventi maggiori di 2 KB, li divide in due pacchetti che vengono consegnati utilizzando la connessione socket. Se il receiver stabilisce che l'evento è parziale, attende per il tempo specificato da questa parola chiave prima di richiamare il secondo pacchetto e completare il processo. Se il secondo pacchetto non è stato ricevuto entro questo periodo di tempo, l'evento parziale ricevuto viene eliminato e viene scritto un messaggio nel file di registro.

APAR: IY52323

Problema: quando un sistema viene riavviato non vengono chiuse le connessioni socket inutilizzate tra agenti Tivoli Risk Manager.

Soluzione: attualmente le connessioni socket inutilizzate vengono automaticamente chiuse.

APAR IY53525

Problema: su sistemi UNIX, il monitor eventi non legge il nuovo file di registro creato quando il file di registro viene ruotato.

Soluzione: attualmente il monitor eventi legge correttamente i nuovi file di registro.

APAR IY53527

Problema: è richiesta la documentazione per la sintassi delle espressioni regolari supportate dal monitor eventi.

Soluzione: il supporto per le espressioni regolari è stato migliorato e la documentazione è stata fornita. Per le modifiche della documentazione, consultare la sezione Aggiornamenti della documentazione.

APAR: IY53678

Problema: il monitor eventi genera un'eccezione di puntatore nullo Java quando analizza gli eventi che corrispondono al modello di indice per una classe, ma non al modello di classe definito per tale classe nel file XML.

Soluzione: l'elaborazione del monitor eventi è stata modificata in modo che se una stringa di eventi corrisponde al modello di indice per una classe ma non al modello di classe, non viene considerata una corrispondenza per tale classe e la ricerca continua.

APAR: IY53713

Problema: viene ricevuta un'eccezione di chiave duplicata quando un gruppo di eventi viene inserito in un database e l'inserimento riesce solo parzialmente.

Soluzione: attualmente l'inserimento di eventi in un database viene effettuato correttamente. Ogni evento viene inserito una sola volta. Se viene identificata una chiave duplicata, l'evento duplicato viene eliminato.

APAR: IY54408

Problema: un utilizzo ripetuto del comando **wrmadmin -i** causa l'arresto del sistema per insufficienza di memoria.

Soluzione: il comando **wrmadmin -i** ora può essere usato ripetutamente senza problemi di memoria.

APAR: IY54568

Problema: il monitor eventi del registro eventi Windows rielabora eventi già elaborati.

Soluzione: gli eventi non vengono rielaborati ripetutamente.

APAR: IY55241

Problema: i file network IDS devono essere aggiornati per includere le firme corrette per la vulnerabilità CAN-2002-0562.

Soluzione: il file delle firme è aggiornato e ora include le firme corrette.

APAR: IY55319

Problema: il comando **wrmqueue** non viene completato quando viene accodato un elevato numero di eventi.

Soluzione: per correggere tale problema sono stati modificati i processi interni collegati al comando **wrmqueue**. Per ulteriori informazioni su tale comando, consultare la sezione Aggiornamenti della documentazione.

APAR IY55895

Problema: *IBMTivoli Risk Manager Guida per gli adattatori* e altri documenti in formato PDF forniti con i diversi pacchetti di adattatori fanno riferimento alla tabella di mappatura eventi. Tale tabella non è pubblicata sul sito Web per cui non è possibile né scaricarla né utilizzarla per riferimento.

Soluzione: il documento relativo alla tabella di mappatura eventi (DCF 1171204) è attualmente pubblicato nel sito Web di supporto di Risk Manager:
http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliRiskManager.html.

APAR IY55927

Problema: durante l'esecuzione in una locale DBCS, l'agente Tivoli Risk Manager elimina gli eventi che contengono caratteri DBCS. Nel registro messaggi di Tivoli Risk Manager viene scritto il seguente messaggio:

HRMAG0135W An event integration facility TECAgent filtered the following event

Soluzione: l'agente Tivoli Risk Manager attualmente elabora correttamente gli eventi che contengono caratteri DBCS.

APAR: IY56431

Problema: il database eventi di Tivoli Risk Manager non supporta Microsoft SQL se è stato installato con l'opzione maiuscole/minuscole. I seguenti sintomi indicano tale problema:

?? Gli eventi non vengono scritti nell'archivio eventi di Microsoft SQL.

?? Nel registro messaggi di Tivoli Risk Manager viene scritto il seguente messaggio:

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

[SQLServer]Invalid object name ‘RM_T_ARC41’

Soluzione: immettere il seguente comando per eseguire il file DDL che corregge tale problema:

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

4 Limitazioni note

Questa sezione fornisce una descrizione di ciascuna limitazione e dell'eventuale soluzione, se disponibile.

4.1 Installazione

Limitazione: durante l'installazione viene visualizzato il seguente messaggio di avvertenza non corretto:

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

(No such file or directory)

Soluzione: se si sospettano errori durante l'installazione, installare nuovamente il prodotto Tivoli Risk Manager e specificare nel comando di installazione la seguente opzione per creare il registro in una directory diversa da /opt/RISKMGR:

-l !*<percorso completo>*

La variabile *<percorso completo>* è il percorso completo del file rminstall_log.txt.

4.2 Server di correlazione

Limitazione: gli eventi dell'agente Tivoli Risk Manager (ad esempio RM_Sensor, RM_Error, RMAgent_Inactive e RMAgent_QueueProblem) non vengono inviati al prodotto Tivoli Enterprise Console e non vengono visualizzati nella console eventi. Tale problema riguarda solo sistemi che soddisfano *entrambi* i criteri seguenti:

?? L'installazione è un server eventi o un server di correlazione distribuito.

?? Non è stata eseguita un'installazione predefinita. Si è scelto di inviare al server Tivoli Enterprise Console solo eventi relativi agli incidenti (RM_Incident). Per ulteriori informazioni sulle scelte relative all'installazione, consultare le pagine 102 e 114 del manuale *Tivoli Risk Manager Installation Guide*, Versione 4.2.

Soluzione: per risolvere tale problema, utilizzare la seguente procedura:

1. Modificare il file $RMADHOME/etc/rmagent.xml sul server eventi e sul server di correlazione e aggiungere la seguente definizione di filtro:

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

2. Modificare la definizione di connettore esistente cambiando l'istruzione <withfilter name ="incidents"/> per specificare un nuovo nome filtro nonSensorEvents come di seguito descritto:

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

3. Riavviare l'agente per applicare le modifiche.

4.3 Server eventi Tivoli Enterprise Console

Limitazione: non appena vengono inviati alla console eventi, gli eventi RMAgent_Inactive e RMAgent_QueueProblem vengono visualizzati nella vista gruppo RM_SensorEvent mescolati ad altri eventi del sensore. Se è stata distribuita la configurazione predefinita per la console eventi Tivoli o i server di correlazione distribuiti, la vista gruppo RM_SensorEvent potrebbe contenere troppi eventi. Ciò rende difficile riconoscere

eventi dell'agente Tivoli Risk Manager che avvertono circa eventuali problemi relativi alle code o all'agente Tivoli Risk Manager nella rete.

Soluzione: per facilitare il monitoraggio dei problemi dell'agente, utilizzare la seguente procedura per personalizzare la vista gruppo RM_Error nella console eventi in modo da includere eventi RMAgent_Inactive e RMAgent_QueueProblem:

1. Dalla vista principale della console eventi fare clic su **Windows ? Configuration**.
2. Nel riquadro sinistro fare slic su **Event Groups**.
3. Fare clic su **RM_Error**.
4. Fare clic con il pulsante destro del mouse sulla finestra e selezionare **Create Filter**. Viene visualizzata la finestra Add Event Group Filter.
5. Nel campo Name, digitare RM_AgentProblem.
6. Nel campo Description, digitare una descrizione facoltativa del filtro.
7. Fare clic su **Add Constraint**.
8. Selezionare **Class** dall'elenco degli attributi.
9. Selezionare **Like** dall'elenco degli operatori.
10. Digitare RMAgent_% per il valore (questo valore è sensibile al maiuscolo/minuscolo).
11. Fare clic su **OK**.
12. Dalla finestra Add Event Group Filter fare clic su **Test SQL** per stabilire se il filtro genera il numero corretto di eventi.
13. Fare clic su **OK** per salvare le modifiche.
14. Arrestare e riavviare la console eventi.
15. Fare clic su **Windows ? Summary Chart View** e aprire il gruppo della console RM_Error per verificare il corretto funzionamento del filtro.

4.4 Agente Tivoli Risk Manager

?? Limitazione: vincoli di memoria possono causare problemi dovuti a memoria insufficiente. Tale problema si verifica più frequentemente su sistemi AIX. Ciò può accadere quando è aumentato il numero di receiver o sender, o viene aggiunto il parametro **instanceCount** a ciascuna definizione di destinazione rmagent.xml. Tale problema si può verificare anche su altre piattaforme se viene aggiunta una grande quantità di sender o un elevato numero di **instanceCounts**, perché entrambe le opzioni causano la generazione di thread aggiuntivi e l'incremento dell'utilizzo della memoria.

L'agente Tivoli Risk Manager è un processo Java ed è vincolato dalle allocazioni di memoria dell'ambiente Java. Su AIX, tale limite di memoria è influenzato dai valori predefiniti di allocazione di memoria nel file /etc/security/limits particolarmente bassi. Per consentire l'esecuzione di Tivoli Risk Manager in un'installazione AIX predefinita, il valore massimo della memoria Java è stato intenzionalmente limitata dal parametro **RmagentMemMax**, definito nel file RMADHOME/etc/rmad.conf. Su AIX, tale valore è impostato su 92 MB, valore appena sufficiente all'installazione di base del server.

Soluzione: il parametro **RmagentMemMax** può essere utilizzato su qualsiasi piattaforma per aumentare il valore massimo di memoria disponibile per Tivoli Risk Manager. Ad esempio, su AIX, procedere come segue:

1. Aumentare i valori predefiniti per data, rss e stack nel file limits (oppure utilizzare il comando **ulimit**)
2. Aumentare il valore di RmagentMemMax nel file rmad.conf.
3. Disconnettersi e riconnettersi al sistema.
4. Immettere il comando **wrmadmin -r** per riavviare l'agente Tivoli Risk Manager.

?? Limitazione: il prodotto Tivoli Risk Manager non può essere riavviato se il disco in cui risiede la directory permanente è pieno.

Soluzione: assicurarsi che lo spazio su disco sia sufficiente prima di riavviare il prodotto Tivoli Risk Manager. Per determinare la quantità richiesta di spazio su disco, utilizzare la seguente formula:

(1 + numero di destinazioni) x 20 MB

Il *numero di destinazioni* è il numero di destinazioni definito nel file rmagent.xml.

?? Limitazione: se il primo carattere di un attributo di evento è un singolo apice, l'evento è danneggiato perché il singolo apice e l'ultimo carattere dell'attributo vengono rimossi. L'esempio seguente mostra un apice iniziale specificato per l'attributo di evento msg e il risultato:

'myHostname' is acting suspiciously

La corrispondente colonna MSG nella tabella archivio conterrà:

myHostname' is acting suspiciousl

Soluzione: evitare, se possibile, di utilizzare un singolo apice negli attributi di evento. Non esiste altra soluzione.

4.5 Risoluzione DNS

Limitazione: per Solaris, il comando **wrmdns** non avvia la risoluzione DNS.

Soluzione: utilizzare la seguente procedura per avviare la risoluzione DNS:

1. Modificare i file summary_engine.conf e incident_engine.conf.
2. Sostituire in entrambi i file la voce dnsResolver=off con dnsResolver=on.
3. Immettere il seguente comando per riavviare l'agente Tivoli Risk Manager:
   wrmadmin -r

4.6 Registrazione di messaggi e tracce

?? Limitazione: in alcuni sistemi Linux, potrebbe non essere possibile modificare dinamicamente le impostazioni del livello di traccia e registro perché le impostazioni predefinite del filtro IP e della protezione firewall sono molto restrittive.

Il pacchetto JLog incluso nel prodotto Tivoli Risk Manager fornisce la maniera di modificare dinamicamente le impostazioni di traccia e registro durante l'esecuzione dell'agente Tivoli Risk Manager. Per ulteriori informazioni su tale funzione, consultare la sezione Logging Command Line Interface del manuale *IBM Tivoli Risk Manager Problem Determination Guide.*

Quando viene avviato, l'agente Tivoli Risk Manager richiama JLog Log Manager che crea un server comandi di registro in attesa sulla porta 9992. Il programma client **logcmd** comunica con il server comandi di registro tramite tale porta. Su alcuni sistemi Linux, la porta 9992 non attende quando l'agente Tivoli Risk Manager è in esecuzione e i comandi **logcmd** non riescono con eccezione Java ConnectionException. Ciò è causato dal filtro IP e dalla protezione firewall installati. Se uno dei seguenti programmi è installato su un sistema Linux e non è possibile verificare se la porta 9992 è in attesa quando viene avviato l'agente di Tivoli Risk Manager, il firewall IP impedisce l'accesso alla porta:

- ?? lokkit
- ?? ipchains
- ?? iptables
- ?? ipfwadm

Soluzione: per la procedura di sblocco della porta 9992 fare riferimento alla documentazione del sistema Linux. Se, per ragioni di sicurezza, si desidera mantenere la porta bloccata, non vi sono interferenze con la registrazione dell'agente Tivoli Risk Manager standard, ma non è possibile modificare dinamicamente le impostazioni di traccia.

?? Limitazione: su sistemi UNIX, i file di registro ruotati vengono compressi, per cui non possono essere letti dall'adattatore IDS dell'host.

Soluzione: per evitare tale problema, disabilitare la funzione di compressione della registrazione per i file di registro ruotati più recenti.

?? Limitazione: il seguente messaggio (HRMAG0147I) non sempre segue immediatamente il messaggio ripetuto:

The previous message was repeated {n} times

In tal caso non esiste la possibilità di stabilire quale messaggio è stato ripetuto.

Soluzione: non è disponibile alcuna soluzione.

4.7 Componente Network IDS

Limitazione: potrebbe non essere possibile avviare il componente Network IDS su sistemi AIX a 32 bit. Ciò può verificarsi perché il dispositivo /dev/bpf0, necessario al componente Network IDS per monitorare la rete, non è definito o non è stato avviato correttamente dopo l'ultimo riavvio del sistema.

Soluzione: definire o ripristinare il dispositivo /dev/bpf0 utilizzando la seguente procedura:

1. Da una sessione di terminale AIX, immettere il comando **tcpdump** .
2. Premere Ctrl+c per terminare il comando **tcpdump** dopo che è stato visualizzato il seguente messaggio, che indica che la connessione Ethernet è stata avviata:

   listening on *xxx*

   Le lettere *xxx* rappresentano il numero del dispositivo Ethernet, ad esempio en0.
3. Immettere i seguenti comandi per arrestare e riavviare il processo Network IDS:

   stopnids

   startnids

4.8 Componente Web IDS

?? Limitazione: la disattivazione del rollover dei file di registro per il componente Web IDS mediante la codifica fileMatch_value=0 nel file webids.cfg causa la visualizzazione di un messaggio di errore.

Soluzione: non esiste alcuna soluzione a tale problema. Il rollover del file di registro non può essere disattivato.

?? Limitazione: il componente Web IDS entra in loop se è configurato per monitorare più server Web sullo stesso sistema e i registri di accesso per i server risiedono tutti nella stessa directory.

Soluzione: memorizzare i registri di accesso dei server Web in directory diverse.

?? Limitazione: il comando **webids -d** non scrive le informazioni di debug sull'output standard (STDOUT). Per ulteriori informazioni, consultare la sezione Aggiornamenti della documentazione.

Soluzione: non è disponibile alcun accorgimento.

4.9 Applicazione Web

?? Limitazione (APAR IY58098): se il sistema in cui è in esecuzione la console Java non è su una sottorete in cui è in esecuzione Websphere Application Server, potrebbe non essere possibile collegarsi alla console Tivoli Risk Manager Web. Ciò si verifica perché lo script rmweb.pl è aggiornato con il nome host breve e non con il nome completo del sistema Web Application Server in esecuzione quando è installata l'applicazione Tivoli Risk Manager Web.

Soluzione: utilizzare la seguente procedura per specificare il nome host completo di Web Application Server:

1. Modificare lo script **rmweb.pl** contenuto nella directory RMADHOME/cgi-bin del server eventi.
2. Individuare la seguente riga (intorno alla riga 47):

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

3. Sostituire il nome host breve nella stringa URL con un nome host completo (ad esempio server1.mycompany.com).

?? Limitazione: se è installata una versione obsoleta di Mozilla, potrebbe non essere possibile utilizzare l'applicazione Web.

Soluzione: installare Mozilla versione 1.7.2 o successiva.

?? Limitazione: dopo la disinstallazione dell'applicazione Web di Tivoli Risk Manager il fornitore JDBC di Tivoli Risk Manager esiste ancora come risorsa WebSphere Application Server.

Soluzione: utilizzare la seguente procedura per rimuovere il fornitore JDBC di Tivoli Risk Manager:

1. Accedere come amministratore alla console amministratore di WebSphere Application Server.
2. Fare clic su **Resources**.
3. Fare clic su **JDBC Providers**.
4. Assicurarsi che l'ambito sia impostato sul livello server.
5. Selezionare la casella di controllo **Risk Manager JDBC Provider**.
6. Fare clic su **Delete**.

?? Limitazione: la guida in linea contiene un riferimento non corretto alla guida per gli indirizzi degli adattatori: quando si fa clic sul punto interrogativo (?) dalla finestra Indirizzi di sistema, il riquadro della guida visualizza le seguenti selezioni per richiamare le informazioni sul sistema:

Indirizzo di origine
Indirizzo di destinazione
Indirizzo sensore
Indirizzo adattatore
Altro

Soluzione: non esiste alcuna soluzione. Non sono disponibili informazioni sull'Indirizzo adattatori.

5 Aggiornamenti della documentazione

Questa sezione fornisce una descrizione degli aggiornamenti della documentazione per la libreria di Tivoli Risk Manager, versione 4.2. Consultare le informazioni contenute nelle sezioni seguenti per conoscere le correzioni da effettuare alla libreria e i miglioramenti funzionali apportati al prodotto Tivoli Risk Manager:

- ?? Aggiornamento di varie documentazioni.
- ?? Funzionamento e gestione delle code
- ?? Documentazione su FFDC e altri tipi di traccia
- ?? Supporto espressioni regolari

5.1 Correzioni relative a varie documentazioni

Questa sezione fornisce informazioni sulle correzioni relative a diverse documentazioni da apportare alla libreria Tivoli Risk Manager e la documentazione di modifiche funzionali di minore importanza apportate a questo fix pack.

5.1.1 IBM Tivoli Risk Manager Administrator's Guide

?? Nella sezione Customizing Incident-Based Correlation Rules, a pag. 101, deve essere aggiunto il seguente testo:

Gli elementi <threshold> e <aggregate> della regola determinano quando generare un incidente. Le regole predefinite fornite con il prodotto Tivoli Risk Manager aggregano eventi cumulando il valore **rm_Level** di ciascun evento del sensore fino a quando viene raggiunto il valore **thresholdCount** ; a tal punto viene generato un incidente. Il valore **rm_Level** rappresenta il peso relativo, o gravità, di ciascun evento. Un metodo alternativo consiste nel contare il numero di eventi e generare un incidente quando il conteggio raggiunge una soglia particolare. Per abilitare il conteggio degli eventi, rimuovere l'elemento <aggregate> dalla regola e regolare il parametro **thresholdCount** in modo che rappresenti il numero di eventi necessario per generare un incidente.

Il parametro **attributeSet** nell'elemento <cloneable> della regola determina quali dell'evento sono utilizzati per aggregare gli eventi in arrivo come candidati per un possibile incidente. I tre attributi di correlazione standard utilizzati in tale parametro sono una qualsiasi combinazione degli attributi**rm_SourceToken**, **rm_DestinationToken**e**rm_CategoryToken**. Di seguito è riportato un elenco di nomi di attributi disponibili che possono essere specificati nel parametro **attributeSet** . Se non altrimenti specificato, il nome dell'attributo utilizzato nella regola è lo stesso di quello degli eventi in arrivo.

- ?? rm_SensorToken
- ?? rm_SourceToken
- ?? rm_DestinationToken
- ?? rm_CategoryToken (sinonimo per rm_ClassCategory)
- ?? rm_CategoryDescription (sinonimo per rm_ClassCategoryDescription)
- ?? rm_CustomerID
- ?? rm_Signature
- ?? rm_Timestamp32
- ?? rm_Level

?? È necessario effettuare la seguente modifica alla sezione Setting an Attribute to a Specific Value, a pag. 103:

L'elemento <parameters> nell'elemento <action> di una regola può essere utilizzato per modificare il valore di ciascun attributo di eventi RM_Incident, ad eccezione degli attributi hostname e msg.

Il secondo esempio a pag. 103 assegna l'attributo msg; tale esempio è errato è deve essere eliminato.

?? Il primo paragrafo della sezione Resource IDs and Dynamic Data a pag. 125 deve essere modificato come segue:

Resource IDs and Dynamic Data: Il testo visualizzato in queste aree è specificato da testo non modificabile o da un ID risorsa.

La codifica non modificabile del testo rappresenta un modo semplice di codificare il testo, in quanto è necessario aggiornare un solo file senza dover arrestare e riavviare il prodotto WebSphere per applicare le modifiche. Tenere presente che se si utilizza Tivoli Risk Manager con un pacchetto di localizzazione, è necessario utilizzare il metodo dell'ID risorsa.

Per utilizzare il testo non modificabile, iniziare e terminare la stringa di testo con &quot.. Utilizzare la seguente procedura per codificare il testo.

1. Modificare il file AdvisorRules.xml.
2. Aggiungere la seguente riga al file:

   title="&quot.View CVE Recommendation &quot."

3. Salvare il file AdvisorRules.xml.

Quando viene visualizzata la pagina Web, nell'area del titolo viene visualizzato *View CVE Recommendations*.

In un testo non modificabile è possibile anche utilizzare dati dinamici, codificando una variabile nella stringa che specifichi un attributo di evento o di incidente. Ad esempio, per visualizzare il valore dell'attributo rm_Category in un testo non modificabile, il testo al passo 2 dovrebbe essere codificato come segue:

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

Il resto della sezione Resource IDs and Dynamic Data a pag. 125 rimane invariato. Esaminare queste informazioni per approfondimenti sui dati dinamici e sugli ID risorsa.

?? La sezione Filtering attributes a pag. 47 deve essere modificata come segue:

Filtro degli attributi

È possibile filtrare gli attributi in modo che non siano inviati al server di Tivoli Enterprise Console.

È possibile aggiungere nel file eif_sender.conf sul proprio agente e sul proprio server di correlazione distribuito un'opzione di configurazione in modo da non inviare alcuni slot estesi al server di Tivoli Enterprise Console.

Ad esempio, aggiungere al file eif_sender.conf la seguente riga:

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

Un esempio di applicazione di filtro è riportato nel file RMADHOME /etc/templates/sensorevent_attributeFilter.xml.

?? La seguente parola chiave deve essere documentata nell'appendice A, Event Intergation Facility Sender and Receiver Keywords:

filterAttributes=pathname ...

Specificare il percorso completo di uno o più file XML che contengono specifiche di filtro degli attributi. Le specifiche possono essere utilizzate per eliminare gli attributi estesi da un evento prima che venga trasmesso. Il filtro degli attributi è utile a un sottocomponente del sender di Event Integration Facility che sta inviando eventi al server Tivoli Event Console per eliminare traffico inutile nella rete e migliorare le prestazioni.

Per un esempio di file di specifiche di filtro attributi, consultare il seguente file:

RMADHOME /etc/templates/sensorevent_attributeFilter.xml

ReadRetryInterval=seconds

Specificare il numero di secondi che deve attendere il receiver Event Integration Facility in caso di ricezione di un evento parziale. Se il receiver stabilisce che l'evento è parziale, attende per il tempo specificato da tale parola chiave prima di recuperare il secondo pacchetto e completare il processo. Se il secondo pacchetto non viene ricevuto in tale periodo di tempo, l'evento parziale precedentemente ricevuto viene eliminato e un messaggio viene scritto nel registro. Il valore predefinito è 120 secondi.

?? La sezione Manually Configuring the Event Monitor a pag. 192 fornisce un esempio errato al passo 3. La riga con <source name="monitor_receiver_webids" deve essere sostituita con <source name="monitor_receiver_nids" come di seguito descritto:

```
<!-- 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>
```

?? La sezione Heartbeat Monitoring a pag. 87 deve essere modificata come di seguito descritto:

Tivoli Risk Manager esegue il monitoraggio automatico degli agenti distribuiti nella rete e avverte quando un agente non è più attivo. L'avvertenza è un evento RMAgent_Inactive generato in uno dei server di correlazione. Gli eventi RMAgent_Inactive sono inclusi nel database di Tivoli Enterprise Console e sono visualizzati sulla console. Viene visualizzato il seguente messaggio di avvertenza:

Missing heartbeat for agent: *<nomehost>/<indirizzo ip>*

<nomehost> e *<indirizzo ip>* sono i valori relativi a nome host e indirizzo IP dell'agente che non invia più eventi RMAgent_HeartBeat.

Per impostazione predefinita, ciascun agente è configurato per generare eventi RMAgent_HeartBeat. Ciascun server di correlazione è configurato per monitorare gli eventi RMAgent_HeartBeat e generare eventi RMAgent_Inactive quando un agente smette di inviare regolari eventi RMAgent_HeartBeat. Per impostazione predefinita, sarà creato un evento RM_Sensor per rappresentare ogni agente che genera eventi RMAgent_HeartBeat. Gli eventi RMAgent_HeartBeat generalmente non sono inoltrati al server o al database di Tivoli Enterprise Console.

5.1.2 IBM Tivoli Risk Manager Command Reference

A pag. 125 è stato erroneamente affermato che è possibile utilizzare il comando **webids -d** per scrivere su un outpout standard (STDOUT) informazioni di debug che è possibile indirizzare a un altro file. Tale opzione non funziona correttamente e non deve essere utilizzata.

5.1.3 IBM Tivoli Risk Manager Installation Guide

L'appendice E, Removing components, deve essere aggiornata con l'aggiunta delle seguenti informazioni:

Effettuare le seguenti attività prima di disinstallare componenti di Tivoli Risk Manager:

1. Arrestare tutti gli adattatori di Tivoli Risk Manager.
2. Immettere il comando **wrmadmin -k** per arrestare il prodotto Tivoli Risk Manager.
3. In caso di eliminazione del server eventi, effettuare le seguenti attività:
   a. Immettere uno dei seguenti comandi:
      Per UNIX: **rmcorr_cfg -delete**

      Per Windows: **bash rmcorr_cfg -delete**

      Nota: tale comando effettua le seguenti operazioni:

      ?? Questo comando carica la rule base predefinita. Per utilizzare una rule base personalizzata, caricarla manualmente utilizzando la GUI o il comando **wrb**.

      ?? Arresta e riavvia il server eventi di Tivoli Enterprise Console.

   b. Immettere il comando **wrmadmin -k**.
4. Disinstallare il componente. Per informazioni sul comando da utilizzare per il componente da eliminare, consultare la Tabella 11 a pag. 177.

Note:

1. I file di Tivoli Risk Manager che sono stati modificati o i file degli adattatori che sono stati aggiunti non vengono rimossi dalla directory di Tivoli Risk Manager.

2. Durante la disinstallazione, sul server eventi non vengono rimossi la tabella archivio di Tivoli Risk Manager, le viste di database e i gruppi di eventi della console eventi. Per rimuovere tali componenti, eliminarli manualmente.

5.1.4 IBM Tivoli Risk Manager Problem Determination Guide

Nella sezione Tivoli Management Environment Send Connection Type , pag. 23, devono essere aggiunte le seguenti informazioni:

Se il tipo di trasporto è stato modificato in TME quando è stato reinstallato Tivoli Risk Manager, il valore della parola chiave TMEEndpoint deve essere modificato in true nel file di script/etc/Tivoli/rma_eif_env.sh come di seguito descritto:

```
TMEEndpoint=true
```

5.2 Funzionamento e gestione delle code

Questa sezione fornisce informazioni sui miglioramenti apportati al funzionamento e alla gestione delle code per APAR IY55319. Sono state effettuate modifiche per migliorare la gestione dello spazio su disco utilizzato per le code permanenti. Prima di tali modifiche, se alcuni eventi venivano inseriti in una coda più velocemente di quanto non fossero elaborati per un lungo periodo di tempo, il prodotto Tivoli Risk Manager non funzionava e il motivo non veniva indicato all'amministratore. Per risolvere tale problema, sono stati aggiunti alcuni parametri di configurazione per gestire le code e informare l'amministratore sul relativo stato. Per ulteriori informazioni su tali modifiche, consultare le seguenti variazioni apportate alla sezione Queues and Event Persistence del manuale *IBM Tivoli Risk Manager Administrator' s Guide*:

Persistenza di code e di eventi

Ciascun sottocomponente dell'agente a cui si fa riferimento nel file rmagent.xml come impostazione to in un connettore ha una coda associata all'elaborazione. Gli eventi che il sottocomponente deve elaborare sono inseriti nella coda associata dal sottocomponente specificato come impostazione from nel connettore. Durante l'elaborazione, il sottocomponente elimina gli eventi dalla coda quando è pronto a elaborare eventi.

Informazioni sulla persistenza

La persistenza è controllata dal parametro **persist** nel file rmagent.xml. Per impostazione predefinita, quando gli eventi sono inseriti in una coda sono persistenti su disco. Quando il sottocomponente in fase di elaborazione termina l'attività, l'evento è rimosso dal disco. È possibile configurare sia la coda del componente engine che la coda del componente destinazione in modo che gli eventi non siano persistenti su disco. Consultare attentamente le seguenti informazioni prima di stabilire se rendere gli eventi persistenti.

La seguente tabella fornisce informazioni utili per comprendere la persistenza di un evento:

Descrizione	Persistenza	Nessuna persistenza
Tutti gli eventi vengono scritti su disco	Sì	No
Gli eventi non riusciti vengono scritti su disco	Sì	Sì
Gli eventi accodati vengono scritti su disco (come tentativi di evento non riusciti) quando l'agente viene arrestato.	No	Sì
Gli eventi non riusciti (ripetuti) vengono elaborati quando viene avviato l'agente	Sì	Sì
Gli eventi non riusciti (persistenti) vengono scritti su disco	Sì	Sì

Perché disattivare la persistenza

Se si evita di scrivere i dati dell'evento su disco e di rimuoverli in un secondo momento, l'elaborazione è più veloce.

Perché NON disattivare la persistenza

Il sistema non ha una memoria illimitata disponibile per l'agente. Se gli eventi non sono persistenti su disco, devono essere conservati in memoria. La persistenza su disco consente di evitare la perdita di eventi se una condizione di errore inattesa provoca l'arresto dell'agente. Disattivando la persistenza, i dati dell'evento potrebbero essere perduti.

È consigliabile disattivare la persistenza?

L'opzione di disattivazione della persistenza è sconsigliata. Si consiglia decisamente di utilizzare la persistenza.

Per disattivare la persistenza, modificare il file rmagent.xml e aggiungere persist="no" alla definizione del sottocomponente; ad esempio:

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

Gestione delle code e parametri di controllo

I seguenti parametri opzionali possono essere utilizzati con l'elemento <destination> nel file di configurazione rmagent.xml per controllare il funzionamento e la gestione della coda:

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

La dimensione della coda e la quantità di spazio libero su disco sono valutati quando gli eventi devono essere accodati. Se la dimensione della coda si avvicina alla grandezza specificata dai parametri **queueMaxSize** e **queueThresholdSize**, un evento RMAgent_QueueProblem viene inviato alla console eventi specificata dal parametro **errorRoute** . Il parametro **queueMessageInterval** controlla la frequenza con cui sono inviati eventi di avvertenza sulla coda. Se non deve essere accodato alcun evento o la coda è già in uno degli stati di attesa, la dimensione della coda e lo spazio su disco non sono valutati e non viene generato alcun evento di avvertenza sulla coda.

Le seguenti informazioni forniscono la descrizione di ogni parametro:

queueThresholdSize

- ?? Tale parametro specifica la dimensione che la coda deve raggiungere prima che un evento di avvertenza sia inviato alla console eventi. Il primo evento viene inviato quando tale valore viene raggiunto, mentre ulteriori eventi sono inviati a intervalli di tempo specificati dal parametro **queueMessageInterval** alla console eventi specificata dal parametro **errorRoute** .
- ?? Se la coda raggiunge la dimensione specificata da tale parametro, non arresta l'elaborazione degli eventi per questo sottocomponente.
- ?? Il valore di tale parametro può essere un numero intero compreso tra 0 e 2147483647. Il valore predefinito 0 indica che non esiste alcun limite.
- ?? In tal caso, una coda si trova nello stato Running(THRESHOLD) come visualizzato dal comando **wrmqueue -l** .

queueMaxSize

- ?? Tale parametro specifica il numero massimo di eventi che può contenere una coda. Quando il numero di eventi nella coda si avvicina a tale valore, il componente che sta inviando gli eventi alla coda arresta l'elaborazione e un evento di avvertenza sulla coda viene inviato alla console eventi. Il primo evento viene inviato quando tale valore viene raggiunto, mentre ulteriori eventi sono inviati ad intervalli di tempo specificati dal parametro **queueMessageInterval** alla console eventi specificata dal parametro **errorRoute** . L'intervallo predefinito è 15 minuti.

?? Il valore di tale parametro può essere un numero intero compreso tra 0 e 2147483647. Il valore predefinito 0 indica che non esiste alcun limite. Il valore di tale parametro deve essere maggiore del valore del parametro **queueThresholdsize** .

?? Quando una coda raggiunge la dimensione massima, si trova nello stato Waiting(MAX) come visualizzato dal comando **wrmqueue -l** .

queueMessageInterval

?? Tale parametro specifica il tempo di attesa (in millisecondi) prima dell'invio del nuovo evento di avvertenza sulla coda RMAgent_QueueProblem. Utilizzare tale parametro per limitare il numero di eventi di avvertenza sulla coda inviati quando la dimensione della coda ha superato il valore specificato dal parametro **queueMaxSize** o dal parametro **queueThresholdSize** .

?? Il valore predefinito è 900000 (15 minuti).

errorRoute

?? Tale parametro specifica il componente (generalmente una console eventi) a cui vengono inviati gli eventi di avvertenza sulla coda quando i valori del parametro **queueMaxSize** o del parametro **queueThresholdSize** vengono superati.

?? Gli eventi di avvertenza sulla coda vengono accodati con tutti gli altri eventi per questa route. Utilizzare tale parametro per accelerare l'invio degli eventi di avvertenza sulla coda mediante la definizione di un indirizzo di destinazione separato per la route dell'errore. Ciò garantisce la puntuale consegna dell'evento di avvertenza sulla coda.

?? Possono essere definite più route dell'errore. Gli eventi di avvertenza sulla coda RMAgent_QueueProblem sono inviati a tutte le route dell'errore specificate.

?? Non esiste alcuna route dell'errore predefinita. Se tale parametro non viene specificato, non viene inviato alcun evento di avvertenza sulla coda RMAgent_QueueProblem.

Esempi di utilizzo dei parametri di gestione e controllo della coda.

Questa sezione fornisce un esempio dell'utilizzo dei parametri di gestione e controllo della coda basati sul seguente scenario:

Obiettivi	Parametro utilizzato	Esempio
Assicurarsi che il numero di eventi accodati non superi mai 100 000.	queueMaxSize	queueMaxSize = "100000"
Si desidera che un evento di avvertenza sulla coda sia inviato quando il numero di eventi accodati raggiunge 10 000	queueThresholdSize	queueThresholdSize="10000"
Si desidera che sia inviato un evento di avvertenza sulla coda.	errorRoute	Si veda più avanti per l'esempio.
Si desidera che venga inviato un evento di avvertenza sulla coda ogni minuto.	queueMessageInterval	queueMessageInterval="60000"

I seguenti esempi mostrano tutti i parametri della coda specificati per gli obiettivi di seguito elencati:

```
<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>
```

Esempi di eventi di gestione della coda

Questa sezione fornisce alcuni esempi di eventi di gestione della coda. Tenere presente che vengono illustrati solo eventi parziali.

?? Il seguente evento informa che il numero di eventi accodati ha raggiunto o superato la soglia configurata per la coda specificata dal parametro **queueThresholdSize**.

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

?? Il seguente evento informa che il numero di eventi accodati si avvicina o ha superato il valore massimo configurato per la coda specificato nel parametro **queueMaxSize** .

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

?? Il seguente evento informa che il disco rigido utilizzato per la coda persistente è pieno.

```
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
```

?? Il seguente evento informa che la coda non è riuscita ed è richiesto un intervento manuale.

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

Descrizione del comando wrmqueue -l

La descrizione dell'opzione **-l** del comando **wrmqueue** deve essere modificata nel manuale *IBM Tivoli Risk Manager Command Reference* come di seguito descritto:

l o -list

Tale opzione elenca le informazioni sulle code. L'output è visualizzato in tre sezioni e fornisce le seguenti informazioni secondo l'ordine elencato:

1. Il nome, lo stato e la definizione della coda
2. Il numero di eventi nella coda
3. Il numero di eventi non riusciti

Viene di seguito riportato un un esempio di output di **wrmqueue -l**:

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	xxxxxxxxx	xxxxx.xx
eif_sender1	xxxxxxxxxx	xxxxxxxxx	xxxxx.xx
eif_sender2	xxxxxxxxxx	xxxxxxxxx	xxxxx.xx
eif_sender3	xxxxxxxxxx	xxxxxxxxx	xxxxx.xx
eif_sender4	xxxxxxxxxx	xxxxxxxxx	xxxxx.xx

queue name	# failed
summarization	tttttttttt(rrrrrrrrrr)
eif_sender1	tttttttttt(rrrrrrrrrr)
eif_sender2	tttttttttt(rrrrrrrrrr)
eif_sender3	tttttttttt(rrrrrrrrrr)
eif_sender4	tttttttttt(rrrrrrrrrr)

Le seguenti informazioni descrivono l'output fornito dall'opzione **-l** del comando **wrmqueue** :

Intestazione della colonna	**Descrizione delle informazioni**
queue name	Il nome della coda.
status	Lo stato della coda (e non del componente). Lo stato viene indicato da uno dei seguenti valori: Running — La coda funziona correttamente. Waiting(MAX) — La dimensione massima della coda configurata è stata raggiunta, e tutti i componenti che stanno inviando eventi alla coda sono posti in stato di attesa. Running(THRESHOLD) — La soglia configurata per la dimensione della coda è stata superata. Waiting(DISKFULL) — Il disco su cui sono memorizzati i file persistenti di Tivoli Risk Manager è pieno e l'agente è in attesa che venga liberato spazio. Failed — La coda non è riuscita. Per informazioni sulla soluzione di tale problema consultare il manuale *Tivoli Risk Manager Problem Determination Guide.*
type	Il tipo di componente che sta leggendo eventi da tale coda: ?? engine ?? sender
persist	Indica se gli eventi sono residenti in memoria o memorizzati su un disco rigido.
# queued	Il numero di eventi disponibile per l'elaborazione da parte del componente.
# processed	Il numero di eventi correttamente elaborati a partire dall'ultimo avvio dell'agente.
#/second	Il numero di eventi al secondo elaborati da quando è stato immesso il comando **wrmqueue -l**, o a partire dal riavvio dell'agente se è la prima volta che il comando **wrmqueue -l** è stato immesso.
# failed	*tttttttttt* è il numero totale di eventi che il componente non è riuscito a elaborare a partire dall'ultimo avvio dell'agente. *rrrrrrrrr* è il numero di tentativi che saranno eseguiti da una coda non riuscita quando viene riavviato l'agente.

5.3 Registrazione di messaggi e traccia

Questa sezione fornisce informazioni sulla nuova funzione FFDC (First Failure Data Capture) e su altre modifiche del secondo capitolo del manuale *IBM Tivoli Risk Manager Problem Determination Guide*, Message and Trace Logging and Other Diagnostic Tools.

Registrazione traccia

Il prodotto Tivoli Risk Manager fornisce 3 livelli di dettaglio della traccia. Il livello più basso, DEBUG_MIN, è quello predefinito. A tale livello si tiene traccia solo delle condizioni di errore. Gli altri due livelli, DEBUG_MID e DEBUG_MAX, forniscono maggiori informazioni. I livelli possono essere modificati cambiando i parametri contenuti nel file di configurazione della registrazione, o richiamando l'interfaccia di riga comandi della registrazione. I dati dei registri traccia attualmente sono disponibili solo in Inglese.

Per impostazione predefinita, per memorizzare tutte le informazioni della traccia viene utilizzato un buffer di memoria. In tal modo l'effetto dell'esecuzione della traccia sulle prestazioni del sistema è minimo. Il buffer viene scaricato sul disco solo quando si verifica un'eccezione. È possibile anche configurare la registrazione della traccia direttamente su disco, in modo da memorizzare i dati della traccia senza che debba verificarsi un'eccezione. Per esempi di configurazione della registrazione della traccia, consultare la sezione "Tivoli Risk Manager Agent and Event Monitor Trace Customization" .

Le registrazioni di traccia risiedono nei seguenti file e directory:

?? I registri traccia del programma Tivoli Risk Manager C su sistemi Linux e UNIX risiedono in /usr/ibm/tivoli/common/HRM/logs/<*applicazione*> .error.log. La variabile <*applicazione*> specifica il nome dell'applicazione.

?? I registri traccia del programma Tivoli Risk Manager C su sistemi Windows risiedono in C:\Programmi\ibm\tivoli\common\HRM\logs\<*applicazione*>.error.log. La variabile <*applicazione*> specifica il nome dell'applicazione.

?? I registri traccia del componente agente Tivoli Risk Manager per sistemi Linux e UNIX risiedono in/usr/ibm/tivoli/common/HRM/logs/traceHRM*n*.log.

?? I registri del componente agente Tivoli Risk Manager per sistemi Windows risiedono in C:\Programmi\ibm\tivoli\common\HRM\logs\traceHRM*n*.log.

?? Le utilità di database di Tivoli Risk Manager, wrmdbclose e wrmdbclear, scrivono i record di traccia in file separati: traceHRM_DBClose.log e traceHRM_DBClear.log rispettivamente.

I record di traccia dell'agente e del monitor eventi di Tivoli Risk Manager sono scritte in file numerati progressivamente, denominati traceHRM*n*.log, dove *n* è un numero. Il registratore di traccia scrive fino a 5 file, ognuno di 1 MB. Se i record di traccia scritti superano complessivamente i 5 MB, il file di traccia esegue il ritorno a capo automatico. Questi limiti del file di traccia sono tutti personalizzabili utilizzando il file di configurazione del registratore. Per modificare il numero di file di traccia, utilizzare il parametro **file.trace.maxFiles**. Per modificare la dimensione massima dei file di traccia, utilizzare il parametro **file.trace.maxFileSize**.

La maggior parte dei messaggi di registro vengono scritti sia nel registro messaggi che nel registro traccia. Per assicurarsi che tutti i messaggi siano scritti nella registro traccia, aggiungere il file di traccia a listenerNames per il registratore dei messaggi come di seguito descritto:

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

FFCD (First Failure Data Capture)

FFDC (First Failure Data Capture) è l'istantanea delle informazioni di traccia al momento in cui si è verificata la condizione di errore. Personalizzando la configurazione della registrazione traccia, è possibile indicare al sistema di eseguire un'istantanea della traccia di tutti gli errori o solo di errori selezionati. Ogni istantanea crea un file di traccia univoco che non viene sovrascritto dalle istantanee di traccia successive. Per impostazione predefinita, FFDC non è attivo nel prodotto Tivoli Risk Manager. Può essere attivato modificando la configurazione della registrazione traccia. Per informazioni sulla modifica della configurazione, consultare la sezione "Tivoli Risk Manager Agent and Event Monitor Trace Customization". Le istantanee FFDC sono disponibili solo sull'agente e sul monitor eventi di Tivoli Risk Manager.

I registri FFDC risiedono nei seguenti file e directory:

Su sistemi UNIX: /usr/ibm/tivoli/common/HRM/FFDC/*AAAA.MM.GG*/traceHRM*n*.log

Su sistemi Windows: C:\Programmi \ibm\tivoli\common\HRM\FFDC\ *AAAA.MM.GG*\traceHRM*n*.log

La variabile *AAAA.MM.GG* rappresenta la data in cui è stata eseguita l'istantanea e *n* è il numero che indica la sequenza dell'istantanea in una certa data.

Registrazione XML

Il prodotto Tivoli Risk Manager utilizza le seguenti colonne dei record del registro traccia e messaggi:

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

Esempi

La seguente query visualizza il contenuto del file di registro messaggi in formato ASCII:

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

La seguente query scrive il contenuto dei file di registro traccia in formato HTML in un file esterno:

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

La seguente query scrive le colonne selezionate dei file di registro traccia in formato HTML in un file esterno:

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

La seguente query scrive le colonne dei messaggi di errore selezionate dal file di registro messaggi in formato HTML in un file esterno:

```
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
```

Personalizzazione della traccia del monitor eventi di Tivoli Risk Manager Agent

La registrazione della traccia dell'agente di Tivoli Risk è controllata dai parametri del file di configurazione di registrazione traccia $RMADHOME/etc/RMLogger.properties. Ad esempio, il parametro **rmLogger.trc.level** controlla la quantità di informazioni di traccia raccolte durante l'esecuzione dell'agente. Il parametro **rmLogger.trc.listenerNames** controlla se le informazioni di traccia sono scritte in memoria o in un file su disco. Per aumentare la quantità di registrazioni di traccia eseguite dall'agente, generalmente devono essere modificati tali parametri in modo da raccogliere una maggiore quantità di informazioni e scriverle sul disco appena vengono create.

Esistono due maniere per effettuare modifiche nella configurazione della traccia:

?? In modo permanente modificando i valori del parametro nel file RMLogger.properties e riavviando l'agente

Ad esempio, utilizzare la seguente procedura per aumentare in modo permanente la registrazione della traccia dell'agente:

1. Modificare il file $RMADHOME/etc/RMLogger.properties per cambiare i seguenti parametri:

```
rmLogger.trc.level=DEBUG_MAX
rmLogger.trc.listenerNames=file.trace
```

2. Riavviare l'agente.

?? In modo transitorio modificando i valori di parametro mediante l'interfaccia di riga comandi di registrazione (consultare la sezione “Logging Command Line Interface”). Per effettuare le modifiche utilizzando questo metodo è necessario che l'agente sia in esecuzione, e tali modifiche hanno effetto solo fino a quando l'agente rimane in esecuzione.

Ad esempio, utilizzare la seguente procedura per aumentare temporaneamente la registrazione della traccia dell'agente mentre questo è in esecuzione:

1. Passare alla directory $RMADHOME/logviewer.
2. Inserire i seguenti comandi da questa directory:

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

Quante più informazioni vengono registrate, maggiore diventa la dimensione dei registri traccia. Una volta raggiunto il numero massimo di file di traccia, i dati di traccia più vecchi vengono sovrascritti da quelli più recenti. La configurazione predefinita della traccia è di 5 file di traccia di 1 MB ciascuno. Per aumentare la capacità del file di traccia fino a 10 file da 2 MB ciascuno, immettere i seguenti comandi:

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

Tali impostazioni hanno effetto solo fino a quando l'agente è in esecuzione; l'arresto e il riavvio dell'agente ripristinano i valori predefiniti. Per diminuire la registrazione della traccia dell'agente mentre questo è in esecuzione, immettere i seguenti comandi:

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

Per consentite le istantanee FFCD (First Failure Data Capture), personalizzare la configurazione della traccia come segue:

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

Tutte queste modifiche alla configurazione interessano tutti i componenti dell'agente di Tivoli Risk Manager, incluso il monitor eventi. Se si desidera configurare il monitor eventi in maniera differente dal resto dell'agente, utilizzare rmLogger.trc.monitor invece di rmLogger.trc nel file di configurazione o nell'interfaccia di riga comandi. Ad esempio, per impostare la registrazione della traccia del monitor eventi a un livello medio e scriverla nel relativo file, impostare i seguenti parametri:

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

Immettere il seguente comando per elencare tutti i registratori di traccia definiti nella configurazione:

```
logcmd list rmLogger.trc
```

Immettere il seguente comando per elencare le impostazioni correnti del registratore di traccia:

```
logcmd config rmLogger.trc
```

Immettere il seguente comando per elencare le impostazioni correnti del registratore di traccia del monitor eventi:

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

5.4 Supporto espressioni regolari

Questa sezione fornisce informazioni sui miglioramenti che sono stati apportati al supporto espressioni regolari per APAR IY53527. Le seguenti informazioni sulle espressioni regolari devono essere aggiunte al manuale *IBM Tivoli Risk Manager Administrator's Guide.*:

Supporto espressioni regolari

In IBM Tivoli Risk Manager, Versione 4.2, sono state aggiunte le seguenti nuove funzioni al monitor eventi basato sul supporto delle espressioni regolari in Tivoli Risk Manager.

?? Prefiltri

?? Indici

?? Maggiore capacità di specificare modelli di eventi

Questa nuova funzione migliora le prestazioni generali e semplifica la creazione di file di formato. Attualmente è possibile inserire modelli di eventi nei file di formato come espressioni regolari, oltre ai semplici token di caratteri speciali forniti nei precedenti rilasci.

Per implementare le nuove funzioni, viene utilizzata la libreria espressioni regolari di Xerces. Il motore corrispondenze delle espressioni regolari Xerces è un'implementazione di un motore di espressioni regolari NFA (Non-deterministic Finite Automaton) tradizionale (non POSIX). La libreria supporta la maggior parte dei costrutti di espressioni regolari supportati, come di seguito indicato:

Costrutto	Simbolo	Descrizione	Esempio	Risultato
Classi di caratteri semplici	[ ]	La forma base di una classe di caratteri (o serie di caratteri). Utilizzare questo costrutto per creare una corrispondenza con uno solo di diversi caratteri.	gr[ae]y	Corrisponde a gray o grey
Classi di caratteri negati	[^]	Corrisponde a tutti i caratteri eccetto quelli elencati. Se si digita un accento circonflesso (^) dopo la parentesi quadra di apertura si nega la classe di caratteri.	gr[^ae]y	Non corrisponde né a gray né a grey.
Caratteri ripetuti	? * +	Corrisponde al token precedente nessuna o una volta. Corrisponde al token precedente nessuna o più volte. Corrisponde al token precedente una o più volte.		
Abbreviazioni	\d \D \s \S \w \W	Corrisponde a qualsiasi cifra Corrisponde a qualsiasi carattere che non sia una cifra Corrisponde a qualsiasi carattere corrisponda a uno spazio Corrisponde a qualsiasi carattere che non corrisponde a uno spazio Corrisponde a qualsiasi carattere corrisponda a una lettera: Corrisponde a qualsiasi carattere non corrisponde a una lettera:		
Punto	[.]	Corrisponde a quasi tutti i caratteri. Procedere con cautela utilizzando tale costrutto. Il punto (.) è uno dei metacaratteri più comunemente utilizzato, ma è anche quello più frequentemente usato in modo errato.		
Ancoraggi		Utilizzati per indicare una posizione, non corrispondono a un carattere. Corrispondono a una posizione prima, dopo o tra caratteri e sono		

	^ $	utilizzati per ancorare la corrispondenza di espressioni regolari a una certa posizione. Indica l'inizio di una riga. Indica la fine di una riga.		
Limiti delle parole	\b \B \w \W	Indica i limiti delle parole. Utilizzato per cercare una corrispondenza con l'intera parola. La versione negativa di \b. Utilizzato per le corrispondenze con i caratteri che non rappresentano parole. La versione negativa di '\w'.	\b(is|art)\b	Corrisponde o alla parola is o alla parola art.
Intervalli	[-]	Utilizzato per specificare un intervallo di valori. Tenere presente che è possibile specificare più intervalli all'interno di una classe di caratteri o anche combinare intervalli e singoli caratteri.	[0-9] [0-9a-fxA-FX]	Corrisponde a una singola cifra compresa tra 0 e 9. Corrisponde a una cifra esadecimale o alla lettera X.
Quantificatori	{}	Utilizzare i quantificatori per quantificare ulteriormente le espressioni Anche ?, *, e + sono quantificatori.	{n} {n,} {n,m}	Corrisponde esattamente *n* volte. Corrisponde almeno *n* volte. Corrisponde almeno *n* volte, ma più di *m* volte.
Lookahead	(?=) (?!)	Corrisponde al carattere successivo.	q(?=u) q(?!u)	Corrisponde a una q seguita da una u. Corrisponde a una q non seguita da una u.
Lookbehind	(?<=)	Corrisponde al carattere precedente.	(?<=a)b (?<!a)b	Corrisponde a una lettera b preceduta dalla lettera a. Corrisponde a una lettera b non preceduta dalla lettera a.
Alternanze raggruppate	(a|e) gr[ae]y	Corrisponde a una singola espressione regolare date molte possibili espressioni. Tenere presente che se all'inizio o alla fine di un'espressione viene specificato '(' and')' , la corrispondenza non è correttamente implementata. Ciò è causato da un problema con la libreria Xerces.	gr(a|e)y gr[ae]y (gray|grey)	Corrisponde a gray o grey

La tabella seguente elenca i costrutti che non sono supportati e i costrutti alternativi che possono essere utilizzati.

Costrutto	Descrizione	Costrutto alternativo
Unioni	Specifica una singola classe di caratteri che consiste di due o più classi separate. Un esempio di Unione è [0-4[6-8]], che corrisponde a qualsiasi numero compreso tra 0 e 8 tranne il 5.	Specificare [0-46-8] per ottenere lo stesso risultato evitando le parentesi nidificate.

Intersezioni	Specifica una singola classe di caratteri che corrisponde a un elemento comune. Un esempio di intersezione è [0-4&&[4678]], che corrisponde al numero 4. Le intersezioni sono simili alle unioni e vengono impiegate in circostanze simili.	Utilizzare lo stesso costrutto alternativo specificato per le unioni.
Sottrazioni	Specifica una singola classe di caratteri che corrisponde a qualsiasi elemento eccetto quello comune. La sottrazione è essenzialmente un'intersezione negata. Un esempio di sottrazione è [0-9&&[^345]], che corrisponde a qualsiasi numero compreso tra 0 e 9 ad eccezione di 3, 4 e 5.	Specificare l'espressione in forma positiva. Ad esempio, [0-26-9].

6 File aggiunti o sostituiti

Questa sezione elenca i file nuovi e i file sostituiti in questo fix pack. RMADHOME si riferisce alla directory di installazione di Tivoli Risk Manager, indicata dalla variabile di sistema RMADHOME.

/etc/init.d/rc.rmagent (Solaris e Linux)
/etc/rc.rmagent (AIX)
/etc/Tivoli/rma_eif_env.sh (eliminare LD_ASSUME_KERNEL su Linux SUSE versione 8 e successive)
RMADHOME /bin/rma_webids-init (solo UNIX o Linux)
RMADHOME/bin/RMCAH040201.sys (solo HPUX)
RMADHOME/bin/RMCAL040201.sys (solo Linux)
RMADHOME/bin/RMCAS040201.sys (solo Solaris)
RMADHOME/bin/RMCAW040201.sys (solo Windows)
RMADHOME/bin/RMCAX040201.sys (solo AIX)
RMADHOME/bin/rmEventLog.dll (solo Windows)
RMADHOME/bin/webids[.bat]
RMADHOME/bin/wrmadmin[.exe]
RMADHOME/bin/wrmdns (tutti ad eccezione di Windows e Solaris)
RMADHOME/bin/wrmqueue (tutti ad eccezione di Windows e 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 (solo UNIX o Linux)
RMADHOME/logviewer/logcmd.bat (solo Windows)
RMADHOME/msg_cat/C/rmeif.cat
RMADHOME/nids/templates/rules/www.rules
RMADHOME/reports/rm_ra_03.rpt (solo Windows)
\Program Files/ibm/tivoli/common/HRM/scripts/getpd.bat (solo Windows)
\Program Files/ibm/tivoli/common/HRM/scripts/getpdinfo.bat (solo Windows)
/sbin/init.d/rc.rmagent (HP)
/usr/ibm/tivoli/common/HRM/scripts/getpdinfo (solo UNIX o Linux)

7 Come contattare il supporto software

In caso di problemi con un prodotto Tivoli, fare riferimento al seguente sito Web:
http://www.ibm.com/software/sysmgmt/products/support/

Per contattare il supporto software, consultare IBM Software Support Guide sul seguente sito Web:

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

La guida fornisce informazioni su come contattare il supporto software IBM, a seconda della gravità del problema, e le seguenti ulteriori informazioni:

- ?? Registrazione e idoneità
- ?? Numeri telefonici e indirizzi e-mail, a seconda del paese
- ?? Informazioni da ottenere prima di contattare IBM Software Support

8 Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti.

IBM potrebbe non offrire in altri paesi i prodotti, i servizi o le caratteristiche trattati nella presente pubblicazione. Per informazioni sui prodotti e i servizi attualmente disponibili nel proprio paese, consultare il rappresentante IBM di zona. Ogni riferimento relativo a prodotti, programmi o servizi IBM non implica che possano essere utilizzati esclusivamente quei prodotti, programmi o servizi IBM. Possono essere utilizzati prodotti, programmi o servizi equivalenti purché non violino i diritti di proprietà intellettuale IBM. Tuttavia, è a carico dell'utente valutare e verificare il funzionamento di un prodotto, programma o servizio non IBM.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nella presente pubblicazione. Il possesso di questa pubblicazione non implica la concessione di alcuna licenza su di essi. È possibile inviare richieste di informazioni sulla licenza, per iscritto, a:

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

Per informazioni sulle licenze relative al DBCS (Double-Byte Character Set), rivolgersi al reparto sulla proprietà intellettuale di IBM nel proprio paese o inviare richieste per iscritto a:

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

Il seguente paragrafo non è valido per il Regno Unito o per tutti i paesi le cui leggi nazionali siano in contrasto con le disposizioni in esso contenute: L'INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE QUESTA PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA", SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIABILITA' ED IDONEITA' AD UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, per cui la presente dichiarazione potrebbe non essere a voi applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate su base periodica; tali modifiche saranno incorporate nelle nuove edizioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti e/o modifiche al prodotto o al programma descritto nella presente pubblicazione in qualsiasi momento e senza preavviso.

Tutti i riferimenti a siti Web non IBM contenuti in questo documento sono forniti solo per consultazione. I materiali disponibili presso i siti Web non fanno parte di questo prodotto e l'utilizzo di questi è a discrezione dell'utente.

IBM potrebbe utilizzare o distribuire informazioni fornite in qualsiasi modo ritenga appropriato senza incorrere in alcun obbligo nei confronti dell'utente.

I possessori delle licenze di questo programma che desiderano informazioni allo scopo di consentire: (i) lo scambio di informazioni tra programmi creati in maniera indipendente (incluso questo) e (ii) l'utilizzo reciproco di informazioni scambiate, devono contattare:

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

Tali informazioni potrebbero essere disponibili mediante appropriate clausole e condizioni, incluso, in alcuni casi, il pagamento di un compenso.

Il programma licenziato descritto nella presente pubblicazione e tutti i materiali licenziati disponibili sono forniti da IBM alle condizioni previste dall'IBM Customer Agreement, IBM International Program License Agreement o contratto equivalente.

I dati relativi alle prestazioni contenuti nella presente pubblicazione sono stati acquisiti in un ambiente controllato. I risultati ottenuti in altri ambienti operativi, quindi, possono essere sensibilmente diversi. Sui sistemi a livello dello sviluppo sono state adottate alcune misure e non esiste garanzia che tali misure siano le stesse su tutti i sistemi generalmente disponibili. Inoltre, alcune misurazioni sono state stimate mediante estrapolazione. I risultati effettivi possono variare. Gli utenti della presente pubblicazione devono verificare i dati applicabili al loro ambiente specifico.

Le informazioni riguardanti prodotti non IBM sono state ottenute dai fornitori di tali prodotti, da loro dichiarazioni pubblicate o altri dati disponibili al pubblico. IBM non ha esaminato tali prodotti e non può rispondere con precisione riguardo a prestazioni, compatibilità o altri reclami riguardanti prodotti non IBM. Richieste sulle potenzialità di prodotti non IBM devono essere indirizzate ai fornitori di tali prodotti.

Tutte le dichiarazioni riguardanti orientamenti o scopi futuri di IBM sono soggette a modifiche o ritrattazioni senza alcun preavviso, rappresentando esclusivamente degli obiettivi.

Queste informazioni contengono esempi di dati e report utilizzati in operazioni commerciali giornaliere. Per illustrarli più completamente possibile, gli esempi includono i nomi di soggetti, aziende, marchi e prodotti. Tutti questi nomi sono fittizi e ogni somiglianza a nomi e indirizzi utilizzati da imprese commerciali reali sono del tutto casuali.

LICENZA SUL COPYRIGHT:

Queste informazioni contengono esempi di programmi nella lingua di origine, che illustrano tecniche di programmazione su varie piattaforme operative. È possibile copiare, modificare e distribuire tali esempi di programmi in qualsiasi forma senza oneri da versare a IBM, per utilizzi di sviluppo, vendita o distribuzione di programmi in conformità all'interfaccia di programmazione per piattaforme operative per le quali i programmi di esempio sono scritti. Questi esempi non sono stati esaminati completamente in tutte le condizioni. IBM, quindi, non può garantire l'affidabilità, la funzionalità o il corretto funzionamento di questi programmi. È possibile copiare, modificare e distribuire tali esempi di programmi in qualsiasi forma senza oneri da versare a IBM, per utilizzi di sviluppo, vendita o distribuzione di programmi in conformità all'interfaccia di programmazione IBM.

In caso di visualizzazione della presente documentazione in copia su software, potrebbero non apparire fotografie e illustrazioni a colori.

Marchi registrati

I seguenti termini sono marchi registrati di International Business Machines Corporation negli Stati Uniti e/o in altri paesi:

IBM, il logo di IBM, Tivoli, il logo di Tivoli, AIX, DB2, Tivoli Enterprise Console, TME, pSeries e zSeries sono marchi o marchi registrati di International Business Machines Corporation o Tivoli Systems Inc. negli Stati Uniti e/o in altri paesi.

Linux è un marchio di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Microsoft e Windows sono marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e in altri paesi.

Java e tutti i marchi basati su Java sono marchi di Sun Microsystems, Inc. negli Stati Uniti e/o in altri paesi.

Nomi di altre società, prodotti o servizi possono essere marchi di altre società.

o

Stampato negli Stati Uniti.